Doc
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – MANUAL VOLUME II

2003
PASTA 24

0001
3690-

JU. 493

Switch Tipo 5 doc 6

0002

3690

JU. 493
J

Switch Tipo 5 doc 6

0003
3690

IP Routing

In a typical installation, the VPN Concentrator is connected to the public network through an external router, which routes data traffic between networks, and it might also be connected to the private network through a router.

The VPN Concentrator itself includes an IP routing subsystem with static routing, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First) functions. RIP and OSPF are routing protocols that routers use for messages to other routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic.

Once the IP routing subsystem establishes the data paths, the routing itself occurs at wire speed. The subsystem looks at the destination IP address in all packets coming through the VPN Concentrator, even tunneled ones, to determine where to send them. If the packets are encrypted, it sends them to the appropriate tunneling protocol subsystem (PPTP, L2TP, IPSec) for processing and subsequent routing. If the packets are not encrypted, it routes them in accordance with the configured IP routing parameters.

To route packets, the subsystem uses learned routes first (learned from RIP and OSPF), then static routes, then uses the default gateway. If you do not configure the default gateway, the subsystem drops packets that it cannot otherwise route. The VPN Concentrator also provides a tunnel default gateway, which is a separate default gateway for tunneled traffic only.

You configure static routes, the default gateways, and system-wide OSPF parameters in this section. This section also includes the system-wide DHCP (Dynamic Host Configuration Protocol) parameters. You configure RIP and interface-specific OSPF parameters on the network interfaces; see Configuration | Interfaces.

This section of the Manager also lets you configure VPN Concentrator redundancy using VRRP (Virtual Router Redundancy Protocol). This feature applies to installations of two or more VPN Concentrators in a parallel, redundant configuration. It provides automatic switchover to a backup system in case the primary system is out of service, thus ensuring user access to the VPN. This feature supports user access via IPSec LAN-to-LAN connections, IPSec client (single-user remote-access) connections, and PPTP client connections.

0004
3690

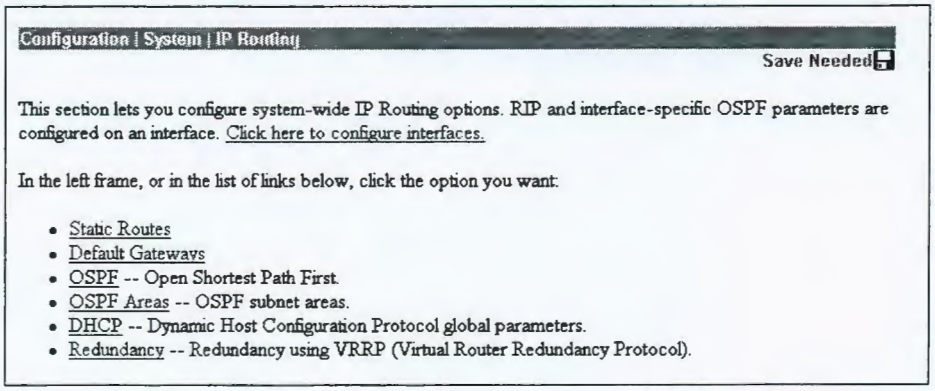
Configuration | System | IP Routing

This section of the Manager lets you configure system-wide IP routing parameters:

- Static Routes: Manually configured routing tables.
- Default Gateways: Routes for otherwise unrouted traffic.
- OSPF: Open Shortest Path First routing protocol.
- OSPF Areas: Subnet areas within the OSPF domain.
- DHCP: Dynamic Host Configuration Protocol global parameters.
- Redundancy: Virtual Router Redundancy Protocol parameters.

You configure RIP and interface-specific OSPF parameters on the network interfaces; click the highlighted link to go to the Configuration | Interfaces screen.

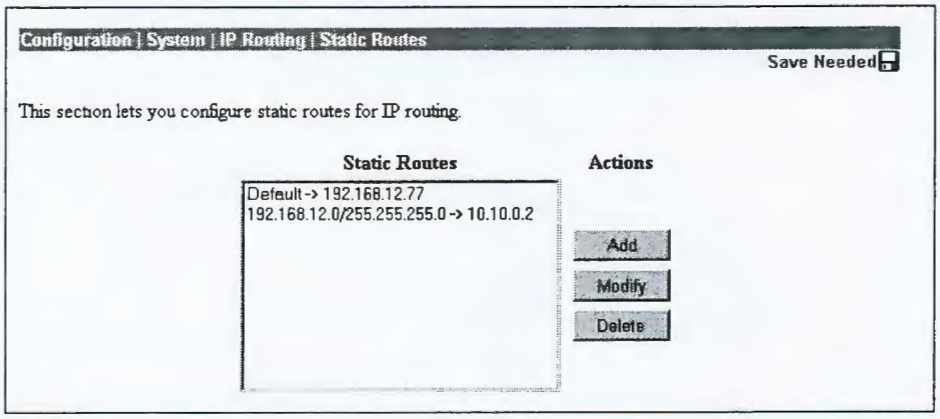
Figure 8-1 Configuration / System / IP Routing Screen



Configuration | System | IP Routing | Static Routes

This section of the Manager lets you configure static routes for IP routing. You usually configure static routes for private networks that cannot be learned via RIP or OSPF.

Figure 8-2 Configuration / System / IP Routing / Static Routes Screen



Static Routes

The Static Routes list shows manual IP routes that have been configured. The format is *[destination network address/subnet mask -> outbound destination]*, for example: 192.168.12.0/255.255.255.0 -> 10.10.0.2. If you have configured the default gateway, it appears first in the list as Default -> default router address. If no static routes have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new static route, click **Add**. The Manager opens the Configuration | System | IP Routing | Static Routes | Add screen.

To modify a configured static route, select the route from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | Static Routes | Modify screen. If you select the default gateway, the Manager opens the Configuration | System | IP Routing | Default Gateways screen.

To delete a configured static route, select the route from the list and click **Delete**.

Note There is no confirmation and no undo.

The Manager refreshes the screen and shows the remaining static routes in the list. You cannot delete the default gateways here; to do so, see the Configuration | System | IP Routing | Default Gateways screen.

Reminder:

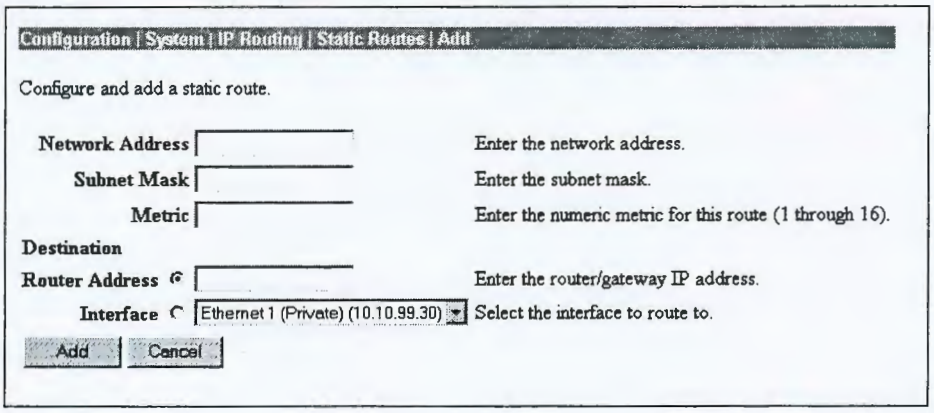
The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | IP Routing | Static Routes | Add or Modify

These Manager screens let you:

- Add: Configure and add a new static, or manual, route to the IP routing table.
- Modify: Modify the parameters for a configured static route.

Figure 8-3 Configuration / System / IP Routing / Static Routes / Add or Modify Screen



Network Address

Enter the destination network IP address to which this static route applies. Packets with this destination address will be sent to the destination you enter. Used dotted decimal notation, for example: 192.168.12.0.

Subnet Mask

Enter the subnet mask for the destination network IP address. Use dotted decimal notation, for example: 255.255.255.0. The subnet mask indicates which part of the IP address represents the network and which part represents hosts. The router subsystem looks at only the network part.

The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.0 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed here, since that would resolve to the equivalent of a default gateway.

Metric

Enter the metric, or cost, for this route. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Destination

Click a radio button to choose the outbound destination for these packets. You can choose only one destination: either a specific router/gateway, or a VPN Concentrator interface.

Router Address

Enter the IP address of the specific router or gateway to which to route these packets; that is, the IP address of the next hop between the VPN Concentrator and the ultimate destination of the packet. Use dotted decimal notation, for example: 10.10.0.2.

Interface

Click the **Interface** drop-down menu button and choose a configured VPN Concentrator interface as the outbound destination. The menu lists all interfaces that have been configured.

For example, in a LAN-to-LAN configuration where remote-access clients are assigned IP addresses that are not on the private network, you could configure a static route with those addresses outbound to the Ethernet 1 (Private) interface. The clients could then access the peer VPN Concentrator and its networks.

Add or Apply / Cancel

To add a new static route to the list of configured routes, click **Add**. Or to apply your changes to a static route, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | IP Routing | Static Routes screen. Any new route appears at the bottom of the Static Routes list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | Static Routes screen, and the Static Routes list is unchanged.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0008
3690

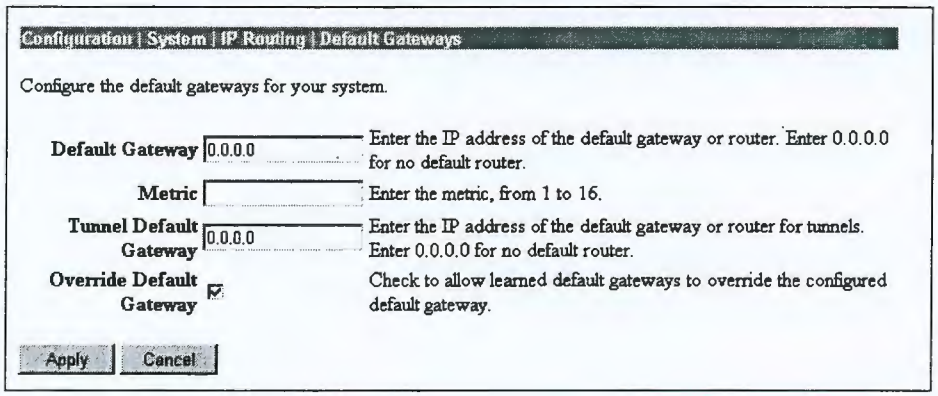
Configuration | System | IP Routing | Default Gateways

This screen lets you configure the default gateway for IP routing, and configure the tunnel default gateway for tunneled traffic. You use this same screen both to initially configure and to change default gateways. You can also configure the default gateway on the Configuration | Quick | System Info screen.

The IP routing subsystem routes data packets first using learned routes, then static routes, then the default gateway. If you do not specify a default gateway, the system drops packets it cannot otherwise route.

For tunneled data, if the system does not know a destination address, it tries to route the packet to the tunnel default gateway first. If that route is not configured, it uses the regular default gateway.

Figure 8-4 Configuration / System / IP Routing / Default Gateways Screen



Default Gateway

Enter the IP address of the default gateway or router. Use dotted decimal notation, for example: 192.168.12.77. This address must *not* be the same as the IP address configured on any VPN Concentrator interface. If you do not use a default gateway, enter 0.0.0.0 (the default entry).

To delete a configured default gateway, enter `0.0.0.0`.

The default gateway must be reachable from a VPN Concentrator interface, and it is usually on the public network. The Manager displays a warning screen if you enter an IP address that is not on one of its interface networks, and it displays a dialog box if you enter an IP address that is not on the public network.

Metric

Enter the metric, or cost, for the route to the default gateway. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if this route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0009
Doc. 3690

Tunnel Default Gateway

Enter the IP address of the default gateway for tunneled data. Use dotted decimal notation, for example: 10.10.0.2. If you do not use a tunnel default gateway, enter `0.0.0.0` (the default entry).

To delete a configured tunnel default gateway, enter `0.0.0.0`.

This gateway is often a firewall in parallel with the VPN Concentrator and between the public and private networks. The tunnel default gateway applies to all tunneled traffic, including IPSec LAN-to-LAN traffic.

Note If you use an external device instead of the VPN Concentrator for NAT (Network Address Translation), you must configure the tunnel default gateway.

Override Default Gateway

To allow default gateways learned via RIP or OSPF to override the configured default gateway, check the **Override Default Gateway** check box (the default). To always use the configured default gateway, uncheck the box.

Apply / Cancel

To apply the settings for default gateways, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen. If you configure a Default Gateway, it also appears in the Static Routes list on the Configuration | System | IP Routing | Static Routes screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0010
Fls. Nº
3690
Doc

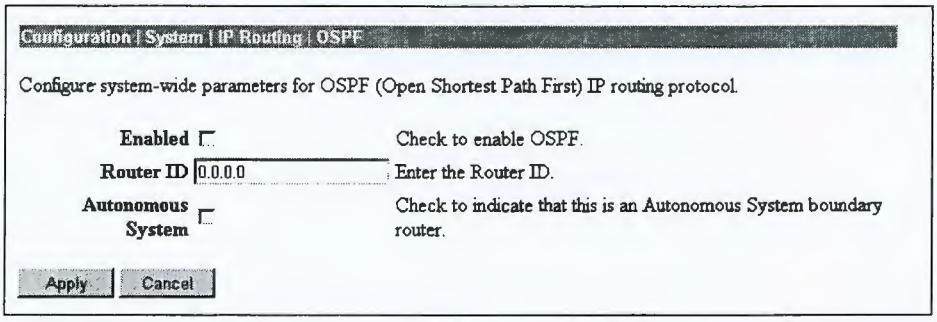
Configuration | System | IP Routing | OSPF

This screen lets you configure system-wide parameters for the OSPF (Open Shortest Path First) routing protocol. You must also configure interface-specific OSPF parameters on the Configuration | Interfaces screens.

OSPF is a protocol that the IP routing subsystem uses for messages to other OSPF routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic. The VPN Concentrator supports OSPF version 2 (RFC 2328).

The complete private network is called an OSPF Autonomous System (AS), or domain. The subnets within the AS are called areas. You configure OSPF areas on the Configuration | System | IP Routing | OSPF Areas screens.

Figure 8-5 Configuration / System / IP Routing / OSPF Screen



Enabled

To enable the VPN Concentrator OSPF router, check the **Enabled** check box. (By default it is unchecked.) You must also enter a Router ID. You must check this box for OSPF to work on any interface that uses it.

To change a configured Router ID, you must disable OSPF here.

To enable OSPF routing on an interface, you must also configure and enable OSPF on the appropriate Configuration | Interfaces screen.

RQS
CPMI
0011
Doc 3690

Router ID

The router ID uniquely identifies the VPN Concentrator OSPF router to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network.

Enter the router ID in the field. Use dotted decimal IP address format, for example: 10.10.4.6. The default entry is 0.0.0.0 (no router configured). If you enable the OSPF router, you must enter an ID.

Note Once you configure and apply a router ID, you must disable OSPF before you can change it. You cannot change the ID back to 0.0.0.0.

Autonomous System

An OSPF Autonomous System (AS), or domain, is a complete internal network. An AS boundary router exchanges routing information with routers belonging to other Autonomous Systems, and advertises external AS routing information throughout its AS.

Check the **Autonomous System** check box to indicate that the VPN Concentrator OSPF router is the boundary router for an Autonomous System. If you check this box, the VPN Concentrator also redistributes RIP and static routes into the OSPF areas. By default, the box is unchecked.

Apply / Cancel

To apply your OSPF settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

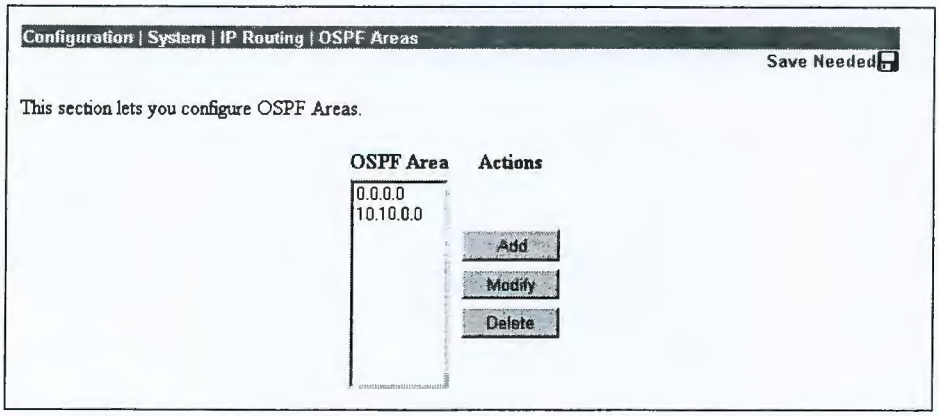
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0012
Doc. 3690

Configuration | System | IP Routing | OSPF Areas

This section of the Manager lets you configure OSPF areas, which are the subnets within an OSPF Autonomous System or domain. You should configure entries for all areas connected to this VPN Concentrator OSPF router.

You can also identify an OSPF area on a VPN Concentrator network interface (see Configuration | Interfaces). Those area identifiers appear in the OSPF Area list on this screen.

Figure 8-6 Configuration / System / IP Routing / OSPF Areas Screen



OSPF Area

The OSPF Area list shows identifiers for all areas that are connected to this VPN Concentrator OSPF router. The format is the same as a dotted decimal IP address, for example: 10.10.0.0. The default entry is 0.0.0.0. This entry identifies a special area known as the backbone that contains all area border routers, which are the routers connected to multiple areas.

Add / Modify / Delete

To configure and add a new OSPF area, click **Add**. The Manager opens the Configuration | System | IP Routing | OSPF Areas | Add screen.

To modify a configured OSPF area, select the area from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | OSPF Areas | Modify screen.

To delete a configured OSPF area, select the area from the list and click **Delete**.

Note There is no confirmation or undo.

The Manager refreshes the screen and shows the remaining entries in the OSPF Area list.

Reminder:

The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

RQS n
CPM
0013
3690
Doc

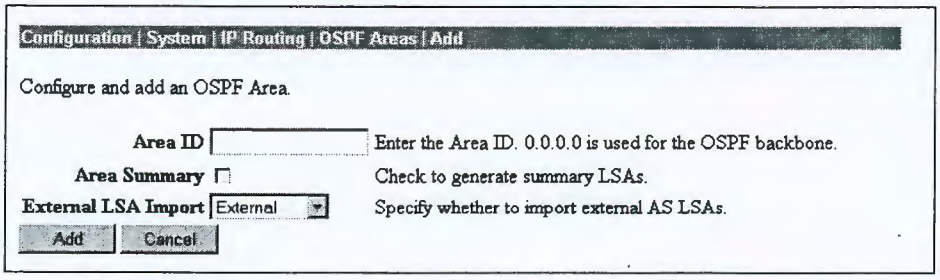
Configuration | System | IP Routing | OSPF Areas | Add or Modify

These Manager screens let you:

- Add: Configure and add an OSPF area.
- Modify: Modify parameters for a configured OSPF area.

Note Once you have configured an OSPF Area, you cannot modify its ID. To change an area ID, delete the existing area and add a new one.

Figure 8-7 Configuration / System / IP Routing / OSPF Areas / Add or Modify Screen



Area ID

- Add: Enter the area ID in the field. Use IP address dotted decimal notation, for example: 10.10.0.0. The default entry is 0.0.0.0, the backbone.
- Modify: Once you have configured an area ID, you cannot change it. See preceding note.

The Area ID identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. The 0.0.0.0 area ID identifies a special area—the backbone—that contains all area border routers.

Area Summary

Check the **Area Summary** check box to have the OSPF router generate and propagate summary LSAs (Link-State Advertisements) into OSPF stub areas. LSAs describe the state of the router's interfaces and routing paths. Stub areas contain only final-destination hosts and do not pass traffic through to other areas. Sending LSAs to them is usually not necessary. By default this box is unchecked.

0014
3690

External LSA Import

Click the **External LSA Import** drop-down menu button and choose whether to bring in LSAs from neighboring Autonomous Systems. LSAs describe the state of the AS router's interfaces and routing paths. Importing those LSAs builds a more complete link-state database, but it requires more processing. The choices are:

- External = Yes, import LSAs from neighboring ASs (the default).
- No External = No, do not import external LSAs.

Add or Apply / Cancel

To add this OSPF area to the list of configured areas, click **Add**. Or to apply your changes to this OSPF area, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | IP Routing | OSPF Areas screen. Any new entry appears at the bottom of the OSPF Area list.

eminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | OSPF Areas screen, and the OSPF Area list is unchanged.

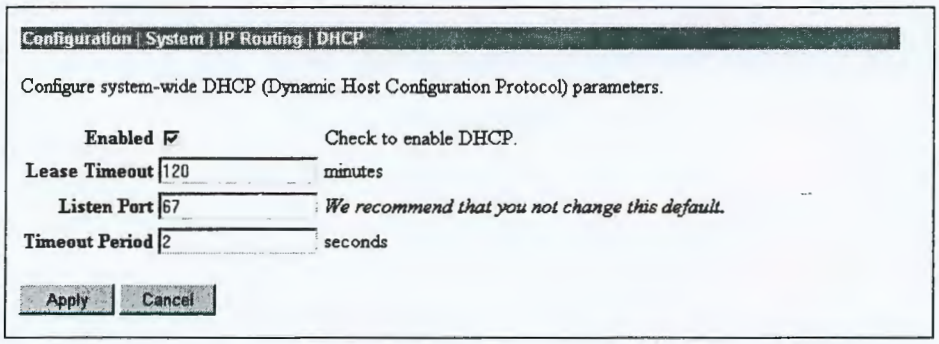
VCS nº 03/2005 - CN
CORREIOS
0015
3690

Configuration | System | IP Routing | DHCP

This screen lets you configure DHCP (Dynamic Host Configuration Protocol) parameters that apply to DHCP functions within the VPN Concentrator. You can use external DHCP servers to assign IP addresses to clients as a VPN tunnel is established.

If you check the Use DHCP check box on the Configuration | System | Address Management | Assignment screen, you must configure at least one DHCP server on the Configuration | System | Servers | DHCP screens. You configure global DHCP parameters here.

Figure 8-8 Configuration / System / IP Routing / DHCP Screen



Enabled

Check the **Enabled** check box to enable DHCP functions within the VPN Concentrator. The box is checked by default. To use DHCP address assignment, you must enable DHCP functions here.

Lease Timeout

Enter the timeout in minutes for addresses that are obtained from a DHCP server. The minimum timeout is 5 minutes. The default is 120 minutes. The maximum is 500000 minutes. DHCP servers "lease" IP addresses for this period of time. Before the lease expires, the VPN Concentrator asks to renew it on behalf of the client. If for some reason the lease is not renewed, the connection terminates when the lease expires. The DHCP server's lease period takes precedence over this setting.

Listen Port

Enter the UDP port number on which DHCP server response messages are accepted. The default is 67, which is the well-known port. *To ensure proper communication with DHCP servers, we strongly recommend that you not change this default.*

Timeout Period

Enter the initial time in seconds to wait for a response to a DHCP request before sending the request to the next configured DHCP server. The minimum time is 1 second. The default time is 2 seconds. The maximum time is 10 seconds. This time doubles with each cycle through the list of configured DHCP servers.

Apply / Cancel

To apply the settings for DHCP parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0017
Doc 3690

Configuration | System | IP Routing | Redundancy

This screen lets you configure parameters for Virtual Router Redundancy Protocol (VRRP), which manages automatic switchover from one VPN Concentrator to another in a redundant installation. Automatic switchover provides user access to the VPN even if one VPN Concentrator is out of service for some reason, for example a system crash, power failure, hardware failure, physical interface failure, system shutdown or reboot.

These functions apply only to installations where two or more VPN Concentrators are in parallel, with the Public interfaces of all systems on a common LAN and with the Private and/or External interfaces of all systems on different common LANs. One VPN Concentrator is the Master system, and the others are Backup systems. A Backup system acts as a virtual Master system when a switchover occurs.

VRRP works only on LAN (Ethernet) interfaces, not on WAN interfaces.

Note If VRRP is configured on a VPN Concentrator, you cannot also enable load balancing. In a VRRP configuration, the backup device remains idle unless the active VPN Concentrator fails. Load balancing does not permit idle devices.

This feature supports user access via IPSec LAN-to-LAN connections, IPSec client (single-user remote-access) connections, and PPTP client connections.

- For IPSec LAN-to-LAN connections, switchover is fully automatic. Users do not need to do anything.
- For single-user IPSec and PPTP connections, users are disconnected from the failing system but they can reconnect without changing any connection parameters.

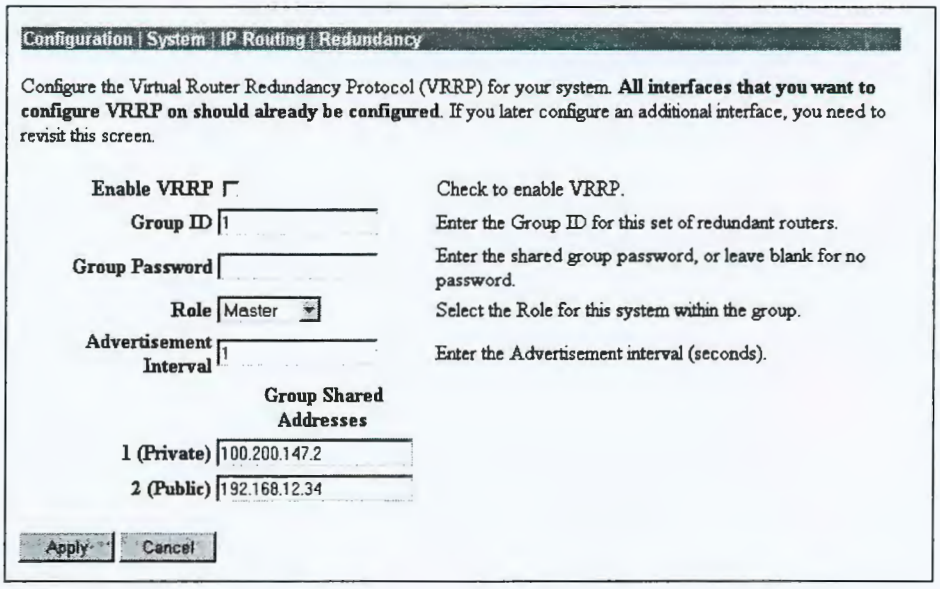
Switchover typically occurs within 3 to 10 seconds.

Note Before configuring or enabling VRRP on this screen, you must configure all Ethernet interfaces that apply to your installation, on all redundant VPN Concentrators. See the Configuration | Interfaces screens.

Note You must also configure *identical* IPSec LAN-to-LAN parameters on the redundant VPN Concentrators. See the Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screens.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0018
Doc 3690

Figure 8-9 Configuration / System / IP Routing / Redundancy Screen



Enable VRRP

Check the **Enable VRRP** check box to enable VRRP functions. The box is unchecked by default.

Group ID

Enter a number that uniquely identifies this group of redundant VPN Concentrators. This number must be the same on all systems in this group. Use a number from 1 (default) to 255. Since there is rarely more than one virtual group on a LAN, we suggest you accept the default.

oup Password

Enter a password for additional security in identifying this group of redundant VPN Concentrators. The maximum password length is 8 characters. The Manager shows your entry in clear text, and VRRP advertisements contain this password in clear text. This password must be the same on all systems in this group. Leave this field blank to use no password.

Role

Click the **Role** drop-down menu button and choose the role of this VPN Concentrator in this redundant group.

- Master = This is the Master system in this group (the default choice). Be sure to configure only one Master system in a group with a given Group ID.
- Backup 1 through Backup 5 = This is a Backup system in this group.

RCS # 03/2001 - CN
CPMI - 0019
3690
Doc 78-13273-01

Advertisement Interval

Enter the time interval in seconds between VRRP advertisements to other systems in this group. Only the Master system sends advertisements; this field is ignored on Backup systems while they remain Backup. The minimum interval is 1 second. The default interval is 1 second. The maximum is 255 seconds. Since a Backup system can become a Master system, we suggest you accept the default for all systems.

Group Shared Addresses

Enter the IP addresses that are treated as configured router addresses by all virtual routers in this group. The Manager displays fields only for the Ethernet interfaces that have been configured.

On the Master system, these entries are the IP addresses configured on its Ethernet interfaces, and the Manager supplies them by default.

On a Backup system, the fields are empty by default, and you must enter the same IP addresses as those on the *Master* system.

1 (Private)

The IP address for the Ethernet 1 (Private) interface shared by the virtual routers in this group.

2 (Public)

The IP address for the Ethernet 2 (Public) interface shared by the virtual routers in this group.

3 (External)

The IP address for the Ethernet 3 (External) interface shared by the virtual routers in this group.

Apply / Cancel

To apply the settings for VRRP, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

0020
3690

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0021
Doc 3690

Switch Tipo 5 doc 7

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0022
Doc 3690

CHAPTER 16

Sessions

Monitoring | Sessions

The following screen shows comprehensive data for all active user and administrator sessions on the VPN Concentrator.

Figure 16-1 Monitoring / Sessions Screen

Monitoring | Sessions — Friday, 24 May 2002 16:48:41

Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group –All–

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
0	0	1	1	1	100	19

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address / Public IP Address	Group	Protocol / Encryption	Login Time / Duration	Client Type / Version	Bytes Tx / Bytes Rx
No Remote Access Sessions						

Management Sessions [LAN-to-LAN Sessions | Remote Access Sessions]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	10.10.98.11	HTTP	None	May 24 16:48:32	0:00:08

78643

0023
3690

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to monitor sessions for that group only. The default value is --All--, which displays sessions for all groups.

0024
3690

Session Summary Table

This table shows summary totals for LAN-to-LAN, remote access, and management sessions.

A session is a VPN tunnel established with a specific peer. In most cases, one user connection = one tunnel = one session. However, one IPSec LAN-to-LAN tunnel counts as one session, but it allows many host-to-host connections through the tunnel.

Active LAN-to-LAN Sessions

The number of IPSec LAN-to-LAN sessions that are currently active.

Active Remote Access Sessions

The number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.

Active Management Sessions

The number of administrator management sessions that are currently active.

Total Active Sessions

The total number of sessions of all types that are currently active.

Peak Concurrent Sessions

The highest number of sessions of all types that were concurrently active since the VPN Concentrator was last booted or reset.

Concurrent Sessions Limit

The maximum number of concurrently active sessions permitted on this VPN Concentrator. This number is model-dependent, for example, model 3060 = 5000 sessions.

Total Cumulative Sessions

The total cumulative number of sessions of all types since the VPN Concentrator was last booted or reset.

14.770

LAN-to-LAN Sessions Table

This table shows parameters and statistics for all active IPSec LAN-to-LAN sessions, initially sorted alphanumerically by connection name. Each session here identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

[Remote Access Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Connection Name

The name of the IPSec LAN-to-LAN connection.

To display detailed parameters and statistics for this connection, click this name. See the Monitoring | Sessions | Detail screen.

IP Address

The IP address of the remote peer VPN Concentrator or other secure gateway that initiated this LAN-to-LAN connection.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 16-1 for definitions of these parameters.

Remote Access Sessions Table

This table shows parameters and statistics for all active remote-access sessions. Each session is a single-user connection from a remote client to the VPN Concentrator. Remote-access sessions include PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions.

Click a column header in this table to sort the table entries in ascending alphanumeric order, using that column as the sort key field.

[LAN-to-LAN Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Username

The username or login name for the session. The field shows `Authenticating...` if the remote-access client is still negotiating authentication. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

To display detailed parameters and statistics for this session, click this name. See the Monitoring | Sessions | Detail screen.

RGS n° 03/2005 - CN
CIOS
File N° 0026
Doc 3690

Public IP Address

The public IP address of the client for this remote-access session. This is also known as the "outer" IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.

Assigned IP Address

The private IP address assigned to the remote client for this session. This is also known as the "inner" or "virtual" IP address, and it lets the client appear to be a host on the private network.

Group

The group name of the client for this remote-access session. Clicking the column head for Group sorts the table entries in ascending alphanumeric order and also sorts the usernames within each group in ascending alphanumeric order.

Client Type and Operating System

The client type of connected clients, and, when available, the associated operating system, sorted by username. For example:

Client Type	Operating System
VPN 3000 Hardware Client	VPN3002
Windows NT client	Windows NT 4.0, Windows 2000, and Windows XP
Windows 98 client	Windows 98
Windows 95client	Windows 95

Version

The software version number (for example, rel. 3.6,_int 50) for connected clients, sorted by username.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 16-1 for definitions of these parameters.

ECT 0027
Doc 3690

Management Sessions Table

This table shows parameters and statistics for all active administrator management sessions on the VPN Concentrator.

[LAN-to-LAN Sessions | Remote Access Sessions]

Click these active links to go to the other session tables on this Manager screen.

Administrator

The administrator username or login name for the session.

IP Address

The IP address of the manager workstation that is accessing the system. Local indicates a direct connection through the Console port on the system.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 16-1 for definitions of these parameters.

Table 16-1 Parameter definitions for Monitoring | Sessions Screen

Parameter	Definition
Protocol	The protocol this session is using. `Console` indicates a direct connection through the Console port on the system. See Monitoring | Sessions | Protocols for a graphical representation of sessions by protocol.
Encryption	The data encryption algorithm this session is using, if any. See Monitoring | Sessions | Encryption for a graphical representation of sessions by encryption algorithm used.
Login Time	The date and time (`MMM DD HH:MM:SS`) that the session logged in. Time is displayed in 24-hour notation.
Duration	The elapsed time (`HH:MM:SS`) between the session login time and the last screen refresh.
Bytes Tx	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Bytes Rx	The total number of bytes received from the remote peer or client by the VPN Concentrator.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0028
Doc 3690

Monitoring | Sessions | Detail

These Manager screens show detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. The parameters and statistics differ depending on the session protocol. There are unique screens for:

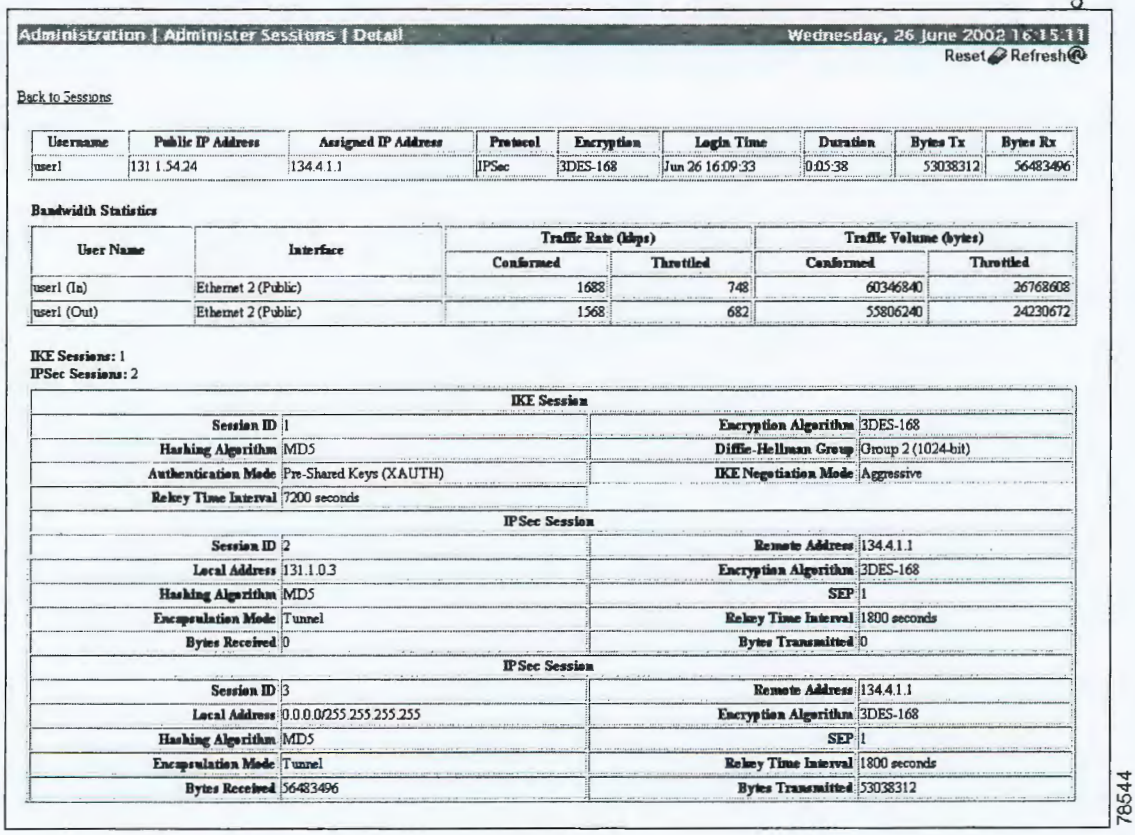
- IPSec LAN-to-LAN (IPSec/LAN-to-LAN)
- IPSec remote access (IPSec User)
- IPSec through UDP (IPSec/UDP)
- IPSec through TCP (IPSec/TCP)
- L2TP
- L2TP over IPSec (L2TP/IPSec)
- PPTP

The Manager displays the appropriate screen when you click a highlighted connection name or username on the Monitoring | Sessions screen. Figure Figure 16-2 shows an example of one kind of detail screen. Depending on the type of connection you select, your detail screen might look somewhat different from the example shown. But, each session detail screen shows three tables: summary data, bandwidth management information, and detail data. The summary data echoes the session data from the Monitoring | Sessions screen. The Bandwidth Statistics table shows information about the effect of policing on that session. The session detail table shows all the relevant parameters for each session and subsession.

See Table 16-2 for definitions of the possible session detail parameters, in alphabetical order.

0029
3690

Figure 16-2 Example of a Monitoring | Sessions | Detail Screen



Administration | Administer Sessions | Detail — Wednesday, 26 June 2002 16:15:11
Reset Refresh

Back to Sessions

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
user1	131.1.54.24	134.4.1.1	IPSec	3DES-168	Jun 26 16:09:33	0:05:38	53038312	56483496

Bandwidth Statistics

User Name	Interface	Traffic Rate (kbps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
user1 (In)	Ethernet 2 (Public)	1688	748	60346840	26768608
user1 (Out)	Ethernet 2 (Public)	1568	682	55806240	24230672

IKE Sessions: 1
IPSec Sessions: 2

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys (XAUTH)	IKE Negotiation Mode	Aggressive
Rekey Time Interval	7200 seconds		
IPSec Session			
Session ID	2	Remote Address	134.4.1.1
Local Address	131.1.0.3	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	1800 seconds
Bytes Received	0	Bytes Transmitted	0
IPSec Session			
Session ID	3	Remote Address	134.4.1.1
Local Address	0.0.0.0/255.255.255.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	1800 seconds
Bytes Received	56483496	Bytes Transmitted	53038312

78544

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back to Sessions

To return to the Monitoring | Sessions screen, click **Back to Sessions**.

RGS nº 03/2006 - CN
CPMI - CORREIOS
0030
3690

Monitoring | Sessions | Detail Parameters

Table 16-2 Parameter Definitions for Monitoring / Sessions / Detail Screens

Parameter	Definition
Assigned IP Address	The private IP address assigned to the remote client for this session. This is also known as the "inner" or "virtual" IP address, and it lets the client appear to be a host on the private network.
Authentication Mode	The protocol or mode used to authenticate this session.
Bytes Rx Bytes Received	The total number of bytes received from the remote peer or client by the VPN Concentrator.
Bytes Tx Bytes Transmitted	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Compression	The data compression algorithm this session is using. LZS is the data compression algorithm used by IPComp. MPPC uses LZ.
Connection Name	The name of the IPSec LAN-to-LAN connection.
Diffie-Hellman Group	The algorithm and key size used to generate IPSec SA encryption keys.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Dynamic Filter	RADIUS user filter applied to this session.
Dynamic Rules	The rules that make up the dynamic filter. For the syntax of these rules, see Dynamic Filters, page 13-3.
Encapsulation Mode	The mode for applying IPSec ESP (Encapsulation Security Payload protocol) encryption and authentication, in other words, what part of the original IP packet has ESP applied.
Encryption Encryption Algorithm	The data encryption algorithm this session is using, if any.
Hashing Algorithm	The algorithm used to create a hash of the packet, which is used for IPSec data authentication.
Idle Time	The elapsed time (HH:MM:SS) between the last communication activity on this session and the last screen refresh.
IKE Negotiation Mode	The IKE (IPSec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	The total number of IKE (IPSec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPSec traffic.
IP Address	The IP address of the remote peer VPN Concentrator or other secure gateway that initiated the IPSec LAN-to-LAN connection.
IPSec Sessions	The total number of IPSec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPSec remote-access session may have two IPSec sessions: one showing the tunnel endpoints, and one showing the private networks reachable through the tunnel.
L2TP Sessions	The total number of user sessions through this L2TP or L2TP / IPSec tunnel; usually 1.

0931
Doc 3690

Table 16-2 Parameter Definitions for Monitoring / Sessions / Detail Screens (continued)

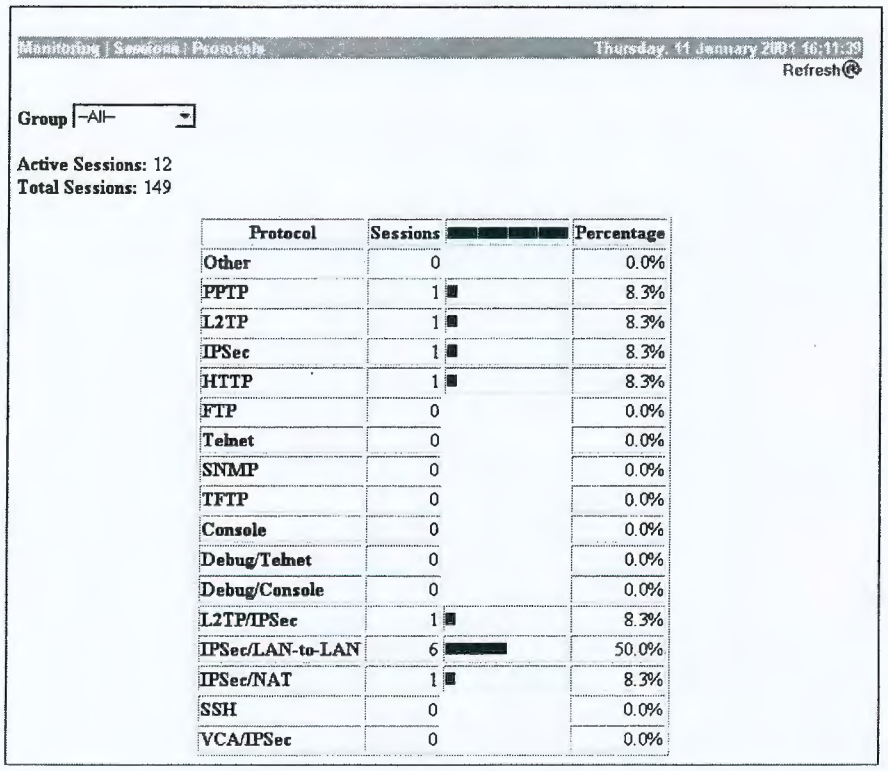
Parameter	Definition
Local Address	The IP address (and wildcard mask) of the destination host (or network) for this session.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Perfect Forward Secrecy Group	The Diffie-Hellman algorithm and key size used to generate IPSec SA encryption keys using Perfect Forward Secrecy.
PFS Group	The Perfect Forward Secrecy group: 1, 2, 3, 4, or 7.
PPTP Sessions:	The total number of user sessions through this PPTP tunnel; usually 1.
Protocol	The tunneling protocol that this session is using.
Public IP Address	The public IP address of the client for this remote-access session. This is also known as the "outer" IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
Rekey Data Interval	The lifetime in kilobytes of the IPSec (IKE) SA encryption keys.
Rekey Time Interval	The lifetime in seconds of the IPSec (IKE) SA encryption keys.
Remote Address	The IP address (and wildcard mask) of the remote peer (or network) that initiated this session.
SEP	The Scalable Encryption Module that is handling cryptographic processing for this session.
Session ID	An identifier for session components (subsessions) on this screen. With IPSec, there is one identifier for each SA.
UDP Port	The UDP port number used in an IPSec through NAT connection.
Username	The username or login name for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

RQS
CPMI
File No. 0032
Doc 3690

Monitoring | Sessions | Protocols

This screen graphically displays the protocols used by currently active user and administrator sessions on the VPN Concentrator.

Figure 16-3 Monitoring / Sessions / Protocols Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show protocols used by currently active users in that group only. The default value is --All--, which displays protocols for users in all groups.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0033
Doc
3690

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

Protocol

The protocol that the session is using:

- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- L2TP = Layer 2 Tunneling Protocol.
- IPSec = Internet Protocol Security tunneling protocol (remote-access users).
- HTTP = Hypertext Transfer Protocol (web browser).
- FTP = File Transfer Protocol.
- Telnet = Terminal emulation protocol.
- SNMP = Simple Network Management Protocol.
- TFTP = Trivial File Transfer Protocol.
- Console = Directly connected console; no protocol.
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- Debug/Console = Debugging via console (for Cisco use only).
- L2TP/IPSec = L2TP over IPSec.
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/UDP = IPSec through NAT (Network Address Translation) via UDP.
- SSH = Secure SHell protocol.
- VCA/IPSec = Virtual Cluster Agent via IPSec. (For Cisco use only.)
- IPSec/TCP = IPSec through NAT (Network Address Translation) via TCP.
- IPSec/NAT-T = IPSec over NAT Traversal.
- IPSec/LAN-to-LAN/NAT-T = IPSec LAN-to-LAN connection over NAT Traversal.
- L2TP/IPSec/NAT-T = L2TP/IPSec connection over NAT Traversal.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0034
Doc 3690

Sessions

The number of active sessions using this protocol. The sum of this column equals the total number of Active Sessions shown above.

Bar Graph

The percentage of sessions using this protocol relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

Percentage

The percentage of sessions using this protocol relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).

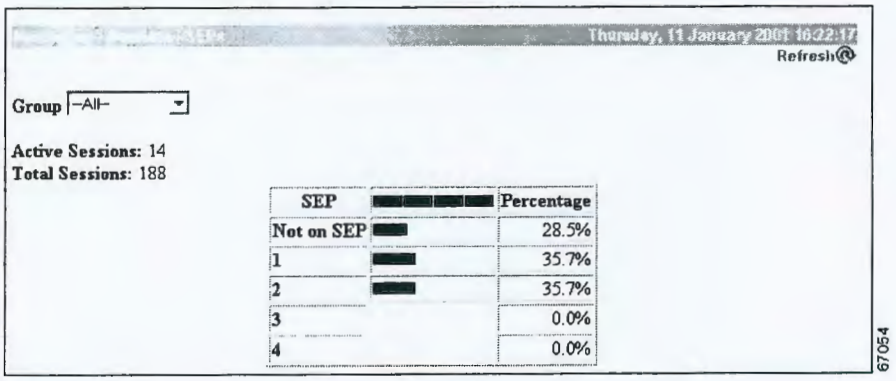
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0035
3690
Doc:

Monitoring | Sessions | SEPs

Note This screen appears on models 3015–3080 only.

This screen graphically displays the SEP (Scalable Encryption Processing) or SEP-E (Enhanced SEP) modules used by currently active user and administrator sessions on the VPN Concentrator. SEP modules perform data encryption functions in hardware.

Figure 16-4 Monitoring | Sessions | SEPs Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to display SEP modules for that group only. The default value is --All--, which displays SEP modules for all groups.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

0036
3690

SEP

The SEP module that the sessions are using.

- Not on SEP = using software encryption, or not using encryption.
- 1, 2, 3, 4 = SEP module 1, 2, 3, and 4, respectively.

Sessions

The number of active sessions using this SEP module. The sum of this column equals the total number of Active Sessions shown above.

Bar Graph

The percentage of sessions using this SEP module relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

Percentage

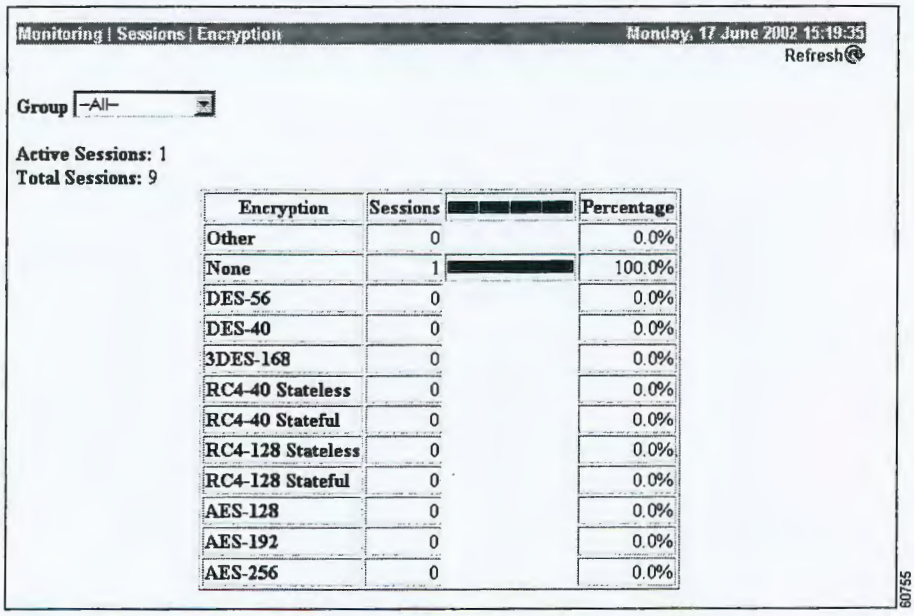
The percentage of sessions using this SEP module relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).

0037
3690

Monitoring | Sessions | Encryption

This screen graphically displays the data encryption algorithms used by currently active user and administrator sessions on the VPN Concentrator.

Figure 16-5 Monitoring | Sessions | Encryption Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to monitor data encryption algorithms used by currently active users in that group only. The default value is --All--, which displays data encryption algorithms for all groups.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

Encryption

The data encryption algorithm that the sessions are using:

- Other = other than listed below.
- None = no data encryption.
- DES-56 = Data Encryption Standard algorithm with a 56-bit key.
- DES-40 = DES encryption with a 56-bit key, 40 bits of which are private.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Sessions

The number of active sessions using this encryption algorithm. The sum of this column equals the total number of Active Sessions shown above.

Bar Graph

The percentage of sessions using this encryption algorithm relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25 percent.

Percentage

The percentage of sessions using this encryption algorithm relative to the total active sessions, as a number. The sum of this column equals 100 percent (rounded).

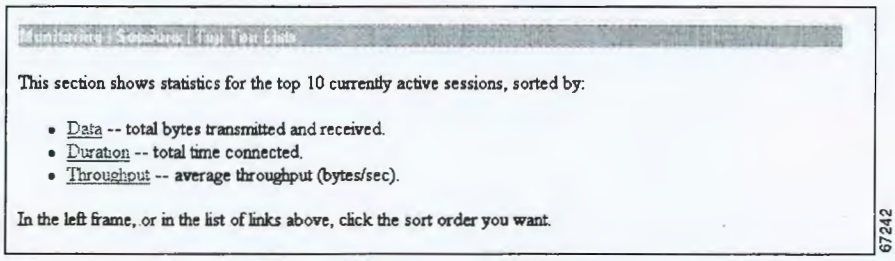
14,757
RQS n° 03003 - CPMI
0039
Fls N°
Doc 3690

Monitoring | Sessions | Top Ten Lists

This section of the Manager shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by:

- Data: total bytes transmitted and received.
- Duration: total time connected.
- Throughput: average throughput (bytes/sec).

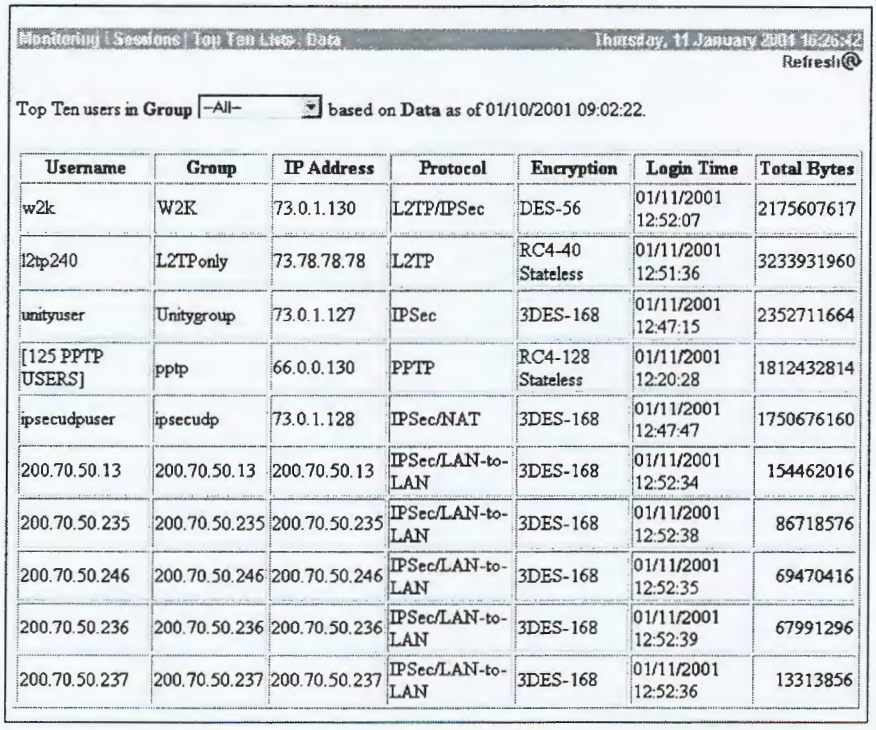
Figure 16-6 Monitoring | Sessions | Top Ten Lists Screen



Monitoring | Sessions | Top Ten Lists | Data

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by data, total bytes transmitted and received.

Figure 16-7 Monitoring / Sessions / Top Ten Lists / Data Screen



Username	Group	IP Address	Protocol	Encryption	Login Time	Total Bytes
w2k	W2K	73.0.1.130	L2TP/IPSec	DES-56	01/11/2001 12:52:07	2175607617
l2tp240	L2TPonly	73.78.78.78	L2TP	RC4-40 Stateless	01/11/2001 12:51:36	3233931960
unityuser	Unitygroup	73.0.1.127	IPSec	3DES-168	01/11/2001 12:47:15	2352711664
[125 PPTP USERS]	pptp	66.0.0.130	PPTP	RC4-128 Stateless	01/11/2001 12:20:28	1812432814
ipsecudpuser	ipsecudp	73.0.1.128	IPSec/NAT	3DES-168	01/11/2001 12:47:47	1750676160
200.70.50.13	200.70.50.13	200.70.50.13	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:34	154462016
200.70.50.235	200.70.50.235	200.70.50.235	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:38	86718576
200.70.50.246	200.70.50.246	200.70.50.246	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:35	69470416
200.70.50.236	200.70.50.236	200.70.50.236	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:39	67991296
200.70.50.237	200.70.50.237	200.70.50.237	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:36	13313856

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show session statistics for that group only. The default value is --All--, which displays session statistics for all groups.

ROS n° 0300[illegible]
CPM [illegible]
0041
Fls N°
Doc 3690

Username

The login username for the session.

Group

The user's group.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using:

- Console = Directly connected console; no protocol.
- Debug/Console = Debugging via console (for Cisco use only).
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- FTP = File Transfer Protocol.
- HTTP = Hypertext Transfer Protocol (web browser).
- IPSec = Internet Protocol Security tunneling protocol (remote-access user).
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/NAT = IPSec through NAT (Network Address Translation).
- L2TP = Layer 2 Tunneling Protocol.
- L2TP/IPSec = L2TP over IPSec.
- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- SNMP = Simple Network Management Protocol.
- Telnet = Terminal emulation protocol.
- TFTP = Trivial File Transfer Protocol.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0042
Fls. Nº
3690
Doc.

14.753

Encryption

The data encryption algorithm that the session is using:

- None = No data encryption.
- DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.
- DES-56 = DES encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Total Bytes

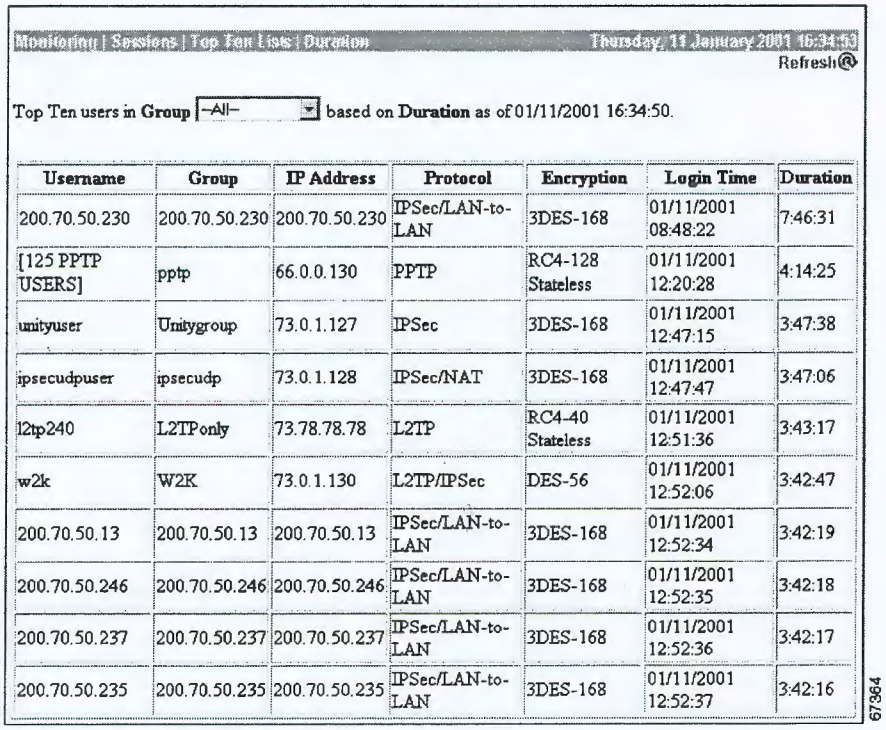
The total number of bytes transmitted and received by this session. N/A = the session is not passing data, in other words, it is an administrator session.

ROS nº 00/0[illegible] - CN
CPMI - CORREIOS
Fls 0043
Doc 3690

Monitoring | Sessions | Top Ten Lists | Duration

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by duration: total time connected.

Figure 16-8 Monitoring | Sessions | Top Ten Lists | Duration Screen



Username	Group	IP Address	Protocol	Encryption	Login Time	Duration
200.70.50.230	200.70.50.230	200.70.50.230	IPSec/LAN-to-LAN	3DES-168	01/11/2001 08:48:22	7:46:31
[125 PPTP USERS]	pptp	66.0.0.130	PPTP	RC4-128 Stateless	01/11/2001 12:20:28	4:14:25
unityuser	Unitygroup	73.0.1.127	IPSec	3DES-168	01/11/2001 12:47:15	3:47:38
ipsecudpuser	ipsecudp	73.0.1.128	IPSec/NAT	3DES-168	01/11/2001 12:47:47	3:47:06
l2tp240	L2TPonly	73.78.78.78	L2TP	RC4-40 Stateless	01/11/2001 12:51:36	3:43:17
w2k	W2K	73.0.1.130	L2TP/IPSec	DES-56	01/11/2001 12:52:06	3:42:47
200.70.50.13	200.70.50.13	200.70.50.13	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:34	3:42:19
200.70.50.246	200.70.50.246	200.70.50.246	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:35	3:42:18
200.70.50.237	200.70.50.237	200.70.50.237	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:36	3:42:17
200.70.50.235	200.70.50.235	200.70.50.235	IPSec/LAN-to-LAN	3DES-168	01/11/2001 12:52:37	3:42:16

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show session statistics for that group only. The default value is --All--, which displays session statistics for all groups.

0044
3690

Username

The login username for the session.

Group

The user's group.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using:

- Console = Directly connected console; no protocol.
- Debug/Console = Debugging via console (for Cisco use only).
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- FTP = File Transfer Protocol.
- HTTP = Hypertext Transfer Protocol (web browser).
- IPSec = Internet Protocol Security tunneling protocol (remote-access user).
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/NAT = IPSec through NAT (Network Address Translation).
- L2TP = Layer 2 Tunneling Protocol.
- L2TP/IPSec = L2TP over IPSec.
- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- SNMP = Simple Network Management Protocol.
- Telnet = Terminal emulation protocol.
- TFTP = Trivial File Transfer Protocol.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0045
Doc 3690

Encryption

The data encryption algorithm that the session is using.

- None = no data encryption.
- DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.
- DES-56 = DES encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Duration

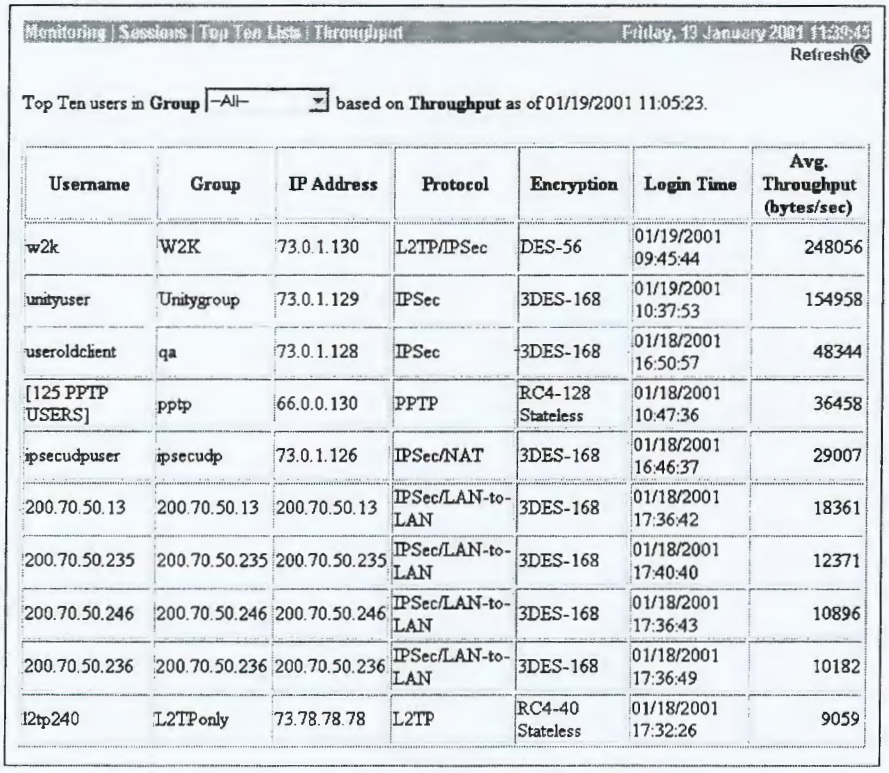
The total amount of time that this session has been connected: HH:MM:SS.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0046
Doc 3690

Monitoring | Sessions | Top Ten Lists | Throughput

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by average throughput (bytes/sec).

Figure 16-9 Monitoring / Sessions / Top Ten Lists / Throughput Screen



Username	Group	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)
w2k	W2K	73.0.1.130	L2TP/IPSec	DES-56	01/19/2001 09:45:44	248056
unityuser	Unitygroup	73.0.1.129	IPSec	3DES-168	01/19/2001 10:37:53	154958
useroldclient	qa	73.0.1.128	IPSec	3DES-168	01/18/2001 16:50:57	48344
[125 PPTP USERS]	pptp	66.0.0.130	PPTP	RC4-128 Stateless	01/18/2001 10:47:36	36458
ipsecudpuser	ipsecudp	73.0.1.126	IPSec/NAT	3DES-168	01/18/2001 16:46:37	29007
200.70.50.13	200.70.50.13	200.70.50.13	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:36:42	18361
200.70.50.235	200.70.50.235	200.70.50.235	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:40:40	12371
200.70.50.246	200.70.50.246	200.70.50.246	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:36:43	10896
200.70.50.236	200.70.50.236	200.70.50.236	IPSec/LAN-to-LAN	3DES-168	01/18/2001 17:36:49	10182
l2tp240	L2TPonly	73.78.78.78	L2TP	RC4-40 Stateless	01/18/2001 17:32:26	9059

efresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Group

Choose a group from the menu to show session statistics for that group only. The default value is --All--, which displays session statistics for all groups.

MCS nº 03/2005 - CN
CPMI - CORREIOS
0047
Doc 3690

Username

The login username for the session.

Group

The user's group.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using:

- Console = Directly connected console; no protocol.
- Debug/Console = Debugging via console (for Cisco use only).
- Debug/Telnet = Debugging via Telnet (for Cisco use only).
- FTP = File Transfer Protocol.
- HTTP = Hypertext Transfer Protocol (web browser).
- IPSec = Internet Protocol Security tunneling protocol (remote-access user).
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
- IPSec/NAT = IPSec through NAT (Network Address Translation).
- L2TP = Layer 2 Tunneling Protocol.
- L2TP/IPSec = L2TP over IPSec.
- Other = Protocol other than those listed here.
- PPTP = Point-to-Point Tunneling Protocol.
- SNMP = Simple Network Management Protocol.
- Telnet = Terminal emulation protocol.
- TFTP = Trivial File Transfer Protocol.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0048
Doc 3690

Encryption

The data encryption algorithm that the session is using.

- None = No data encryption.
- DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.
- DES-56 = DES encryption with a 56-bit key.
- 3DES-168 = Triple-DES encryption with a 168-bit key.
- RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.
- RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.
- RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.
- AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key.
- AES-192 = AES encryption with a 192-bit key.
- AES-256 = AES encryption with a 256-bit key.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Avg. Throughput (bytes/sec)

The average throughput of the session, which is [total bytes transmitted and received] divided by total connect time. N/A = the session is not passing data, in other words, it is an administrator session.

ROF nº 03/2005 - CN
CPMI - CORREIOS
0049
Doc 3690

0050
Doc 3690

1144745

Switch Tipo 5 doc 8

ROS nº 03/2005 - CN
CPMI - CORREIOS
0051
Fls. Nº
Doc 3690

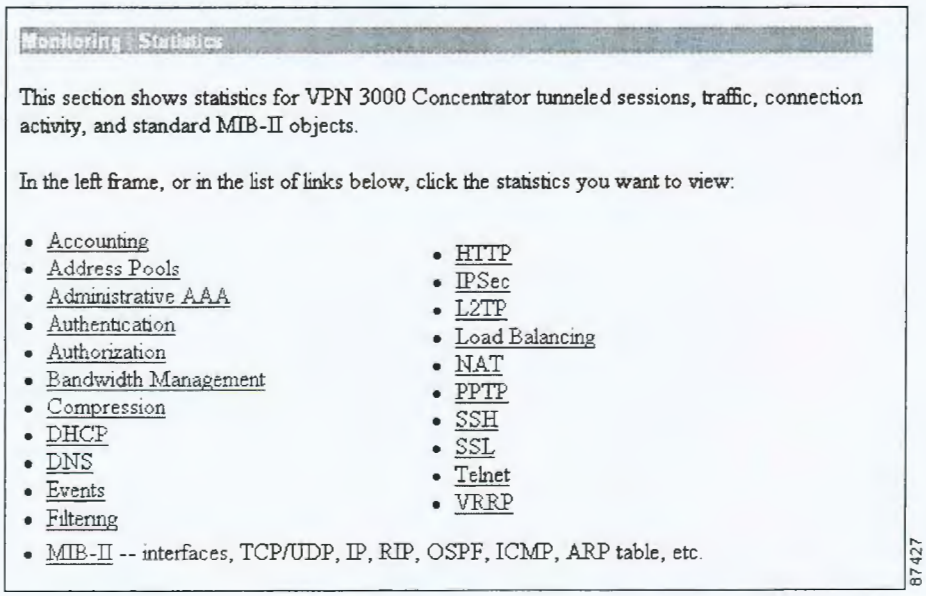
CHAPTER 17

Statistics

Monitoring | Statistics

This section of the Manager shows statistics for traffic and activity on the VPN Concentrator since it was last booted or reset, and for current tunneled sessions, plus statistics in standard MIB-II objects for interfaces, TCP/UDP, IP, ICMP, and the ARP table.

Figure 17-1 Monitoring / Statistics Screen



CORREIOS
0052
3690

J4.743
J

Statistics include:

- Accounting: total requests, responses, timeouts, etc.
- Address Pools: configured pools, allocated and available addresses.
- Administrative AAA: requests, accepts, rejects, challenges, timeouts, etc.
- Authentication: total requests, accepts, rejects, challenges, timeouts, etc.
- Authorization: total requests, accepts, rejects, challenges, timeouts, etc.
- Bandwidth Management: volume and rate of traffic managed by bandwidth policies.
- Compression: pre and post-compression byte totals for IPComp and MPPC.
- DHCP: leased addresses, duration, server addresses, etc.
- DNS: total requests, responses, timeouts, etc.
- Events: total events sorted by class, number, and count.
- Filtering: total inbound and outbound filtered traffic by interface.
- HTTP: total data traffic and connection statistics.
- IPSec: total Phase 1 and Phase 2 tunnels, received and transmitted packets, failures, drops, etc.
- L2TP: total tunnels, sessions, received and transmitted control and data packets; and detailed current session data.
- Load Balancing: device role; device load; and cluster peers' sessions, IP addresses, priority, etc.
- NAT: Network Address Translation session data.
- PPTP: total tunnels, sessions, received and transmitted control and data packets; and detailed current session data.
- SSH: total and active sessions, bytes and packets sent and received, etc.
- SSL: total sessions, encrypted vs. unencrypted traffic, etc.
- Telnet: total sessions, and current session inbound and outbound traffic.
- VRRP: total advertisements, Master router roles, errors, etc.
- MIB-II Stats: interfaces, TCP/UDP, IP, RIP, OSPF, ICMP, ARP table, Ethernet, and SNMP.

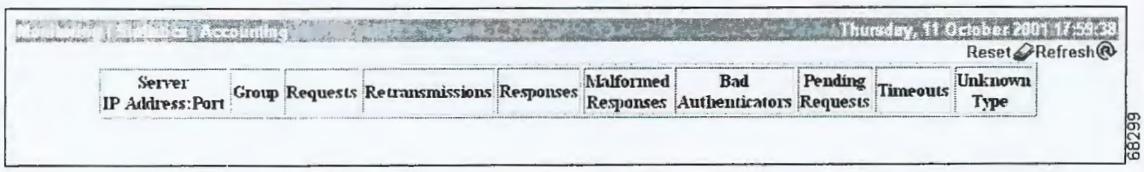
ROS nº 03/2005 - CPI
CPMI - CORREIOS
Fls Nº 0053
Doc 3690

Monitoring | Statistics | Accounting

This screen shows statistics for RADIUS user accounting activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with RADIUS accounting servers, see the Configuration | System | Servers | Accounting screens.

Figure 17-2 Monitoring | Statistics | Accounting Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Server IP Address: Port

The IP address of the configured RADIUS user accounting server, and the port number that the VPN Concentrator is using to access the server. Each configured accounting server is a row in this table. The well-known port number for RADIUS accounting is 1646.

Group

The group on which the server is configured.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0054
Doc 3690

Requests

The number of accounting request packets sent to this RADIUS accounting server. This number does not include retransmissions.

Retransmissions

The number of accounting request packets retransmitted to this RADIUS accounting server.

Responses

The number of accounting response packets received from this RADIUS accounting server.

Malformed Responses

The number of malformed accounting response packets received from this RADIUS accounting server. Malformed packets include packets with an invalid length. Bad authenticators are not included in this number.

Bad Authenticators

The number of accounting response packets received from this server that contained invalid authenticators.

Pending Requests

The number of accounting request packets sent to this RADIUS accounting server that have not yet timed out or received a response.

Timeouts

The number of accounting timeouts to this RADIUS server. After a timeout the system may retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

Unknown Type

The number of RADIUS packets of unknown type received from this server on the accounting port.

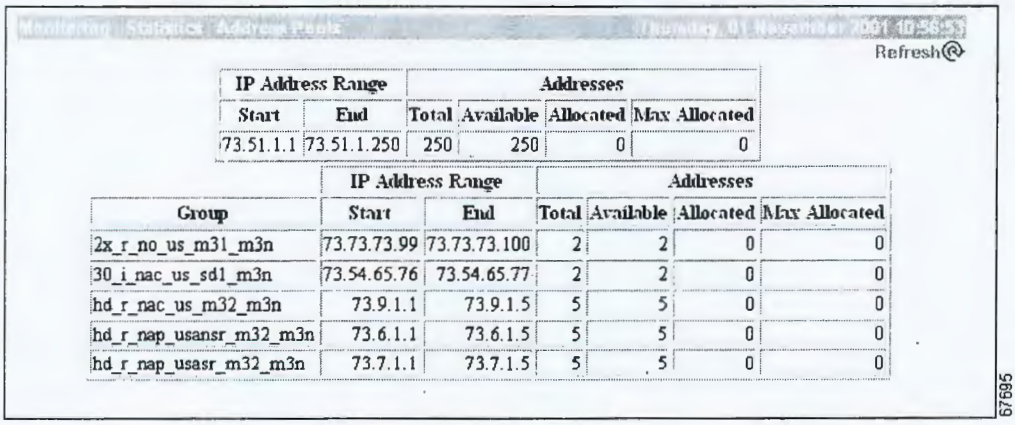
0055
Fls N°
Doc 3690

Monitoring | Statistics | Address Pools

This screen shows statistics for address pool activity on the VPN Concentrator since it was last booted or reset. This data appears if the VPN Concentrator is configured to assign IP addresses to clients from an internal address pool.

To configure address pools, see the Configuration | System | Address Management screens.

Figure 17-3 Monitoring | Statistics | Address Pools Screen



IP Address Range		Addresses			
Start	End	Total	Available	Allocated	Max Allocated
73.51.1.1	73.51.1.250	250	250	0	0

	IP Address Range		Addresses			
Group	Start	End	Total	Available	Allocated	Max Allocated
2x_r_no_us_m31_m3n	73.73.73.99	73.73.73.100	2	2	0	0
30_i_nac_us_sd1_m3n	73.54.65.76	73.54.65.77	2	2	0	0
hd_r_nac_us_m32_m3n	73.9.1.1	73.9.1.5	5	5	0	0
hd_r_nap_usansr_m32_m3n	73.6.1.1	73.6.1.5	5	5	0	0
hd_r_nap_usasr_m32_m3n	73.7.1.1	73.7.1.5	5	5	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IP Address Range: Start / End

The starting and ending IP addresses in the configured address pool. Each configured range is a row in the table.

0056
3690

14.739

Total Addresses

The total number of IP addresses in this configured pool.

Available Addresses

The number of IP addresses available (unassigned) in this pool.

Allocated Addresses

The number of IP addresses currently assigned from this pool.

Max Allocated Addresses

The maximum number of IP addresses assigned from this pool at any one time.

Group

The names of configured groups.

IP Address Range: Start / End

The starting and ending IP addresses in the group's address pool. Each configured range is a row in the table.

Total Addresses

The total number of IP addresses in the address pool of this group.

Available Addresses

The number of IP addresses available (unassigned) in this group's pool.

Allocated Addresses

The number of IP addresses currently assigned from this group's pool.

Max Allocated Addresses

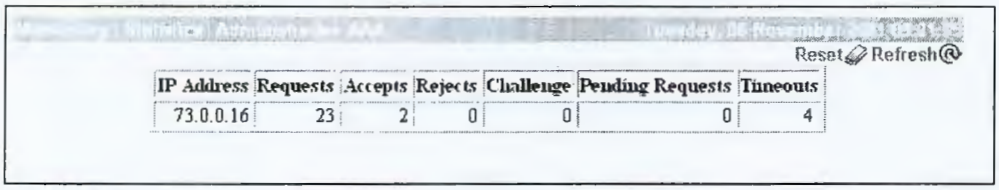
The maximum number of IP addresses assigned from this group's pool at any one time.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0057
3690
Doc

Monitoring | Statistics | Administrative AAA

If you have configured a TACACS+ server, this screen shows statistics for communications between the VPN Concentrator and the TACACS+ server since the VPN Concentrator was last booted or reset.

Figure 17-4 Monitoring | Statistics | Administrative AAA Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IP Address

The IP address of the TACACS+ server.

Requests

The number of requests for authentication, information, or authorization from the VPN Concentrator to the TACACS+ server.

Accepts

The number of successful authentications.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0058
Doc 3690

Rejects

The number of rejected authentications.

Challenge

This field is not used.

Pending Requests

The number of requests that have not yet been answered.

Timeouts

The number of times the VPN Concentrator timed out waiting for a request.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

RGS nº 03/2005 - CN
CPMI - CORREIOS
0059
Fls. Nº
Do 3690

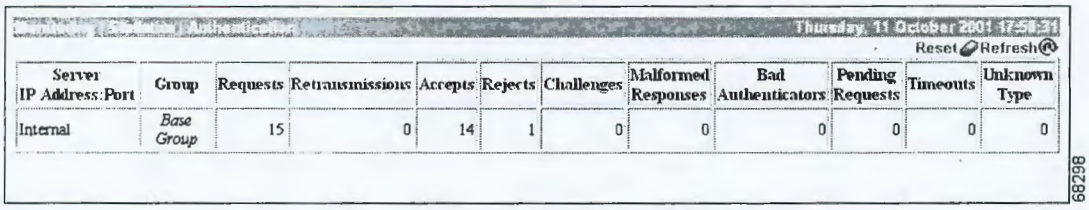
Monitoring | Statistics | Authentication

This screen shows statistics for user authentication activity on the VPN Concentrator since it was last booted or reset.

Note Not all fields apply to all types of authentication servers.

To configure the VPN Concentrator to communicate with authentication servers, see the Configuration | System | Servers | Authentication screens.

Figure 17-5 Monitoring | Statistics | Authentication Screen



Server IP Address:Port	Group	Requests	Retransmissions	Accepts	Rejects	Challenges	Malformed Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Type
Internal	*Base Group*	15	0	14	1	0	0	0	0	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls 0060
Doc 3690

Server IP Address:Port

The IP address of the configured authentication server, and the port number that the VPN Concentrator is using to access the server. Each configured authentication server is a row in this table. Internal identifies the internal VPN Concentrator authentication server.

When the authentication server is an SDI 5.0 server, this field becomes a link. Click the link to view the Monitoring | Statistics | Authentication | Replicas screen, which displays a list of replicas, and data about them (see the next section).

The default, or well-known, port numbers identify an authentication server type:

- 139 = NT Domain
- 389 = LDAP
- 1645 = RADIUS
- 5500 = SDI

Group

The group on which the server is configured.

Requests

The total number of authentication request packets sent to this server. This number does not include retransmissions.

Retransmissions

The number of authentication request packets retransmitted to this server.

Accepts

The number of authentication acceptance packets received from this server.

Rejects

The number of authentication rejection packets received from this server.

Challenges

The number of authentication challenge packets received from this server.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0061
Doc. 3690

14,734

Malformed Responses

The number of malformed authentication response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators are not included in this number.

Bad Authenticators

The number of bad authentication response packets received from this server. Bad authenticators contain invalid authenticators or signature attributes.

Pending Requests

The number of authentication request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authentication timeouts to this server. After a timeout the system might retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

Unknown Type

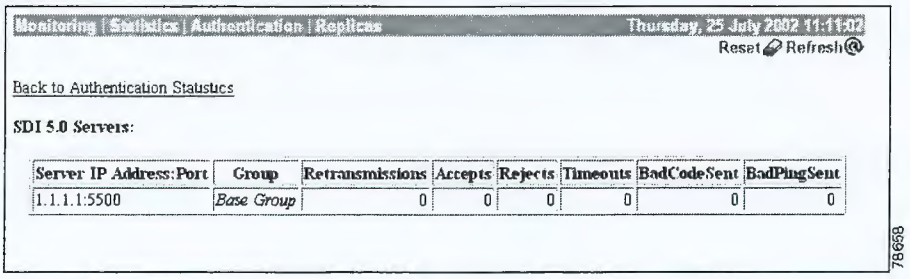
The number of authentication packets of unknown type received from this server.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0062
Doc 3690

Monitoring | Statistics | Authentication | Replicas

This screen shows statistics for SDI 5.0 user authentication activity on the VPN Concentrator since it was last booted or reset.

Figure 17-6 Monitoring | Statistics | Authentication | Replicas Screen



Server IP Address:Port

The IP address of the configured SDI authentication server, and the port number that the VPN Concentrator is using to access the server.

The default, or well-known, port numbers for an SDI 5.0 authentication server is 5500.

Group

The group on which the server is configured.

Retransmissions

The number of authentication request packets retransmitted to this server.

Accepts

The number of authentication acceptance packets received from this server.

Rejects

The number of authentication rejection packets received from this server.

RDS nº 03/2005 - CN
CPMI - CORREIOS
0063
Fls Nº
Doc 3690

Timeouts

The number of authentication timeouts to this server. After a timeout the system might retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

BadCodeSent

The number of bad code packets received from this server. Bad code packets indicate invalid SecurID token code.

BadPinSent

The number of bad pin packets received from this server. Bad pin packets indicate invalid user identification.

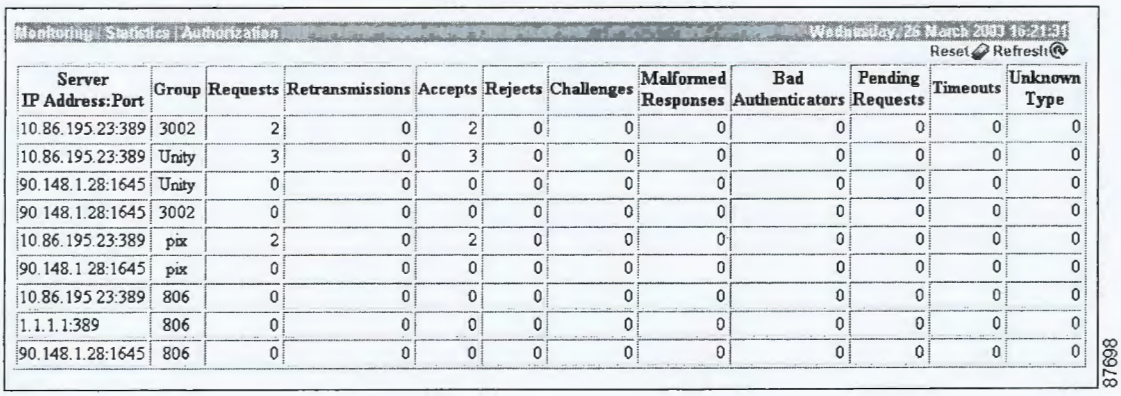
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0064
Doc 3690

Monitoring | Statistics | Authorization

This screen shows statistics for user authorization activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with authorization servers, see the Configuration | System | Servers | Authorization screens.

Figure 17-7 Monitoring | Statistics | Authorization Screen



Server IP Address:Port	Group	Requests	Retransmissions	Accepts	Rejects	Challenges	Malformed Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Type
10.86.195.23:389	3002	2	0	2	0	0	0	0	0	0	0
10.86.195.23:389	Unity	3	0	3	0	0	0	0	0	0	0
90.148.1.28:1645	Unity	0	0	0	0	0	0	0	0	0	0
90.148.1.28:1645	3002	0	0	0	0	0	0	0	0	0	0
10.86.195.23:389	pix	2	0	2	0	0	0	0	0	0	0
90.148.1.28:1645	pix	0	0	0	0	0	0	0	0	0	0
10.86.195.23:389	806	0	0	0	0	0	0	0	0	0	0
1.1.1.1:389	806	0	0	0	0	0	0	0	0	0	0
90.148.1.28:1645	806	0	0	0	0	0	0	0	0	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0065
Fls. Nº
3690
Doc

Server IP Address:Port

The IP address of the configured authorization server, and the port number that the VPN Concentrator is using to access the server. Each configured authorization server is a row in this table. Internal identifies the internal VPN Concentrator authorization server.

The default, or well-known, port numbers identify an authorization server type:

- 389 = LDAP
- 1645 = RADIUS

Group

The group on which the server is configured.

.equests

The total number of authorization request packets sent to this server. This number does not include retransmissions.

Retransmissions

The number of authorization request packets retransmitted to this server.

Accepts

The number of authorization acceptance packets received from this server.

Rejects

The number of authorization rejection packets received from this server.

Challenges

The number of authorization challenge packets received from this server.

Malformed Responses

The number of malformed authorization response packets received from this server. Malformed packets include packets with an invalid length. Bad authorizations are not included in this number.

0066
Fls Nº
3690
Doc

Bad Authenticators

The number of bad authorization response packets received from this server. Bad authenticators contain invalid authenticators or signature attributes.

Pending Requests

The number of authorization request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authorization timeouts to this server. After a timeout the system might retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

Unknown Type

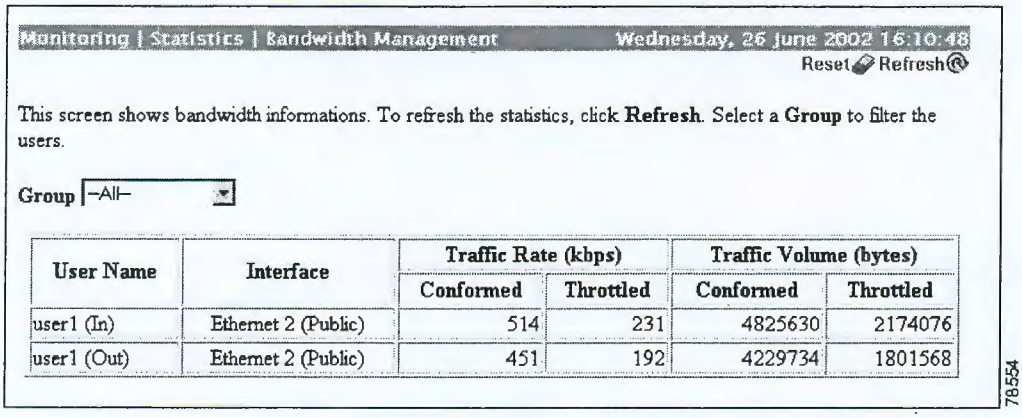
The number of authorization packets of unknown type received from this server.

ECT nº 03/2005 - CN
CPMI - CORREIOS
0067
3690

Monitoring | Statistics | Bandwidth Management

This screen shows details of the effects of bandwidth management policies on each tunnel. Only tunnels on which bandwidth management policies are enabled appear on this screen.

Figure 17-8 Monitoring / Statistics / Bandwidth Management Screen



User Name	Interface	Traffic Rate (kbps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
user1 (In)	Ethernet 2 (Public)	514	231	4825630	2174076
user1 (Out)	Ethernet 2 (Public)	451	192	4229734	1801568

Group

Choose a group from the **Group** menu to show bandwidth statistics for users in that group only. The default value is --All--, which displays bandwidth statistics for users in all groups.

User Name

The user name identifying a tunnel using a bandwidth management policy.

Traffic Rate (kbps)

Conformed

The current rate of session traffic (as set by the bandwidth management policy).

Throttled

The rate at which packets are being throttled to maintain the conformed rate.

ROS nº 03/2005 - CX
CPMI - CORREIOS
Fls. Nº 0068
Doc 3690

Traffic Volume (bytes)

Conformed

The number of bytes of session traffic (as set by the bandwidth management policy).

Throttled

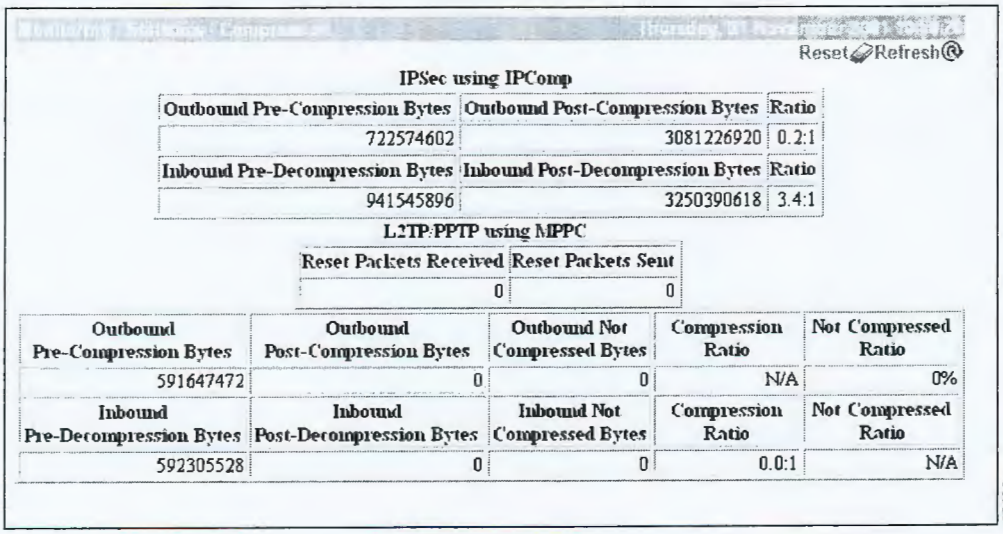
The number of bytes being throttled to maintain the conformed rate.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0069
Doc. 3690

Monitoring | Statistics | Compression

If you have enabled data compression, this screen shows statistics for data compression on the VPN Concentrator since it was last booted or reset.

Figure 17-9 Monitoring | Statistics | Compression Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

0070
Fls. Nº
Doc 3690

IPSec Using IPComp

This screen shows statistics for IPSec data compression using the IPComp compression protocol.

Note The following IPComp statistics measure the results of compression on *all* incoming and outgoing data, including data not intended for compression and data that is not compressible.

Outbound Pre-Compression

The total number of bytes of all outbound data before compression.

Outbound Post-Compression

The total number of bytes of all outbound data after compression.

atio

The ratio of Outbound Pre-Compression to Outbound Post-Compression.

Inbound Pre-Decompression

The total number of bytes of all incoming data before any of it is decompressed.

Inbound Post-Decompression

The total number of bytes of all incoming data after decompression.

Ratio

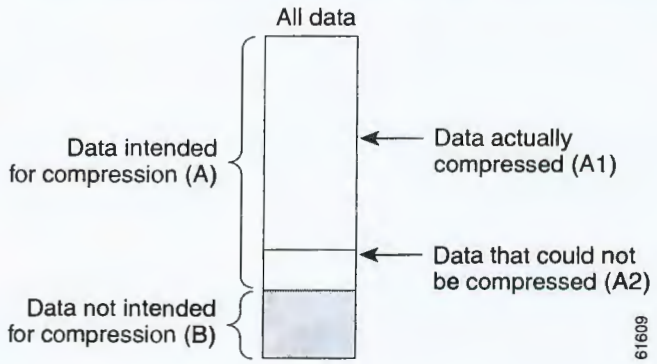
The ratio of Inbound Post-Decompression to Inbound Pre-Decompression.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0071
Doc 3690

L2TP/PPTP Using MPPC

This table shows statistics for L2TP and PPTP data compression using the MPPC compression protocol. These MPPC statistics use the following distinctions. (See Figure 17-10.) All data transmitted can be divided into two groups: data intended for compression (A) and data that is not intended for compression (B). Of the data intended for compression, some of it actually compresses (A1) and some does not (A2). (The compression process would actually cause certain data to expand, so this data is left uncompressed.)

Figure 17-10 Distinctions Used for Data Compression Statistics



Resets Received

The total number of reset requests received from the remote peer.

Resets Sent

The total number of reset requests sent to the remote peer.

Outbound Pre-Compression

The total number of bytes of outbound data intended for compression. ("A" in Figure 17-10.)

Outbound Post-Compression

The total number of bytes of outbound data actually compressed. ("A1" in Figure 17-10.)

Outbound Not Compressed

The total number of bytes of data intended for compression that were not compressed. The compression process would actually cause certain data to expand, so this data is left uncompressed. ("A2" in Figure 17-10.)

Compression Ratio

The ratio of Outbound Pre-Compression to (Outbound Post-Compression + Outbound Not Compressed).

0072
Doc 3690

Not Compressed Ratio

The ratio of Outbound Pre-Compressed to Outbound Not Compressed.

Inbound Pre-Decompression

The total number of bytes of incoming data intended for decompression. ("A" in Figure 17-10.)

Inbound Post-Decompression

The total number of bytes of incoming data actually decompressed. ("A1" in Figure 17-10.)

Inbound Not Compressed

The total number of uncompressed inbound data bytes of the data. ("A2" in Figure 17-10.)

ompression Ratio

The ratio of (Inbound Post-Decompression + Inbound Not Compressed) to Inbound Pre-Decompression.

Not Compressed Ratio

The ratio of Inbound Pre-Decompression to Inbound Not Compressed.

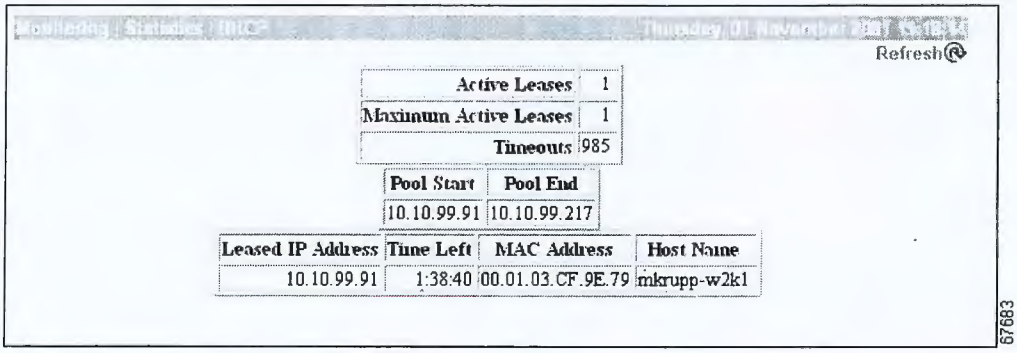
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0073
3690
Doc.

Monitoring | Statistics | DHCP

This screen shows statistics for DHCP (Dynamic Host Configuration Protocol) activity on the VPN Concentrator since it was last booted or reset. Each row of the table shows data for each session using an IP address via DHCP.

To identify DHCP servers to the VPN Concentrator, see Configuration | System | Servers | DHCP. To configure system-wide DHCP functions within the VPN Concentrator, see Configuration | System | IP Routing | DHCP. To use DHCP to assign addresses to clients, see the Configuration | System | Address Management | Assignment screen.

Figure 17-11 Monitoring / Statistics / DHCP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Leased IP Address

The IP address leased from the DHCP server by the remote client.

Fis N° 0074
Doc 3690

Lease Duration

The duration of the current IP address lease, shown as HH:MM:SS.

Time Used

The total length of time that this session has had an active IP address lease, shown as HH:MM:SS.

Time Left

The time remaining until the current IP address lease expires, shown as HH:MM:SS.

DHCP Server Address

The IP address of the DHCP server that leased this IP address.

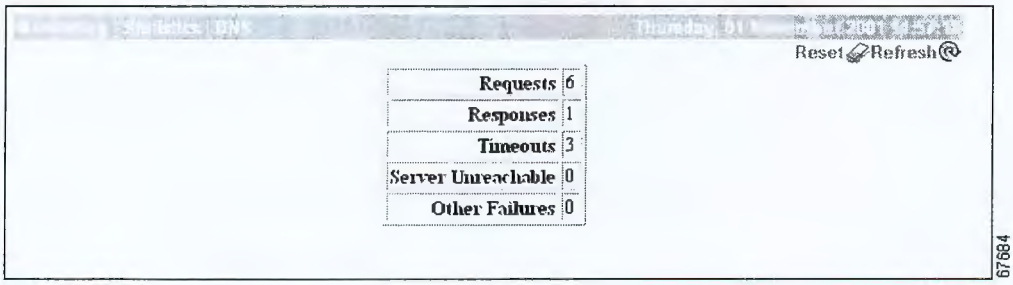
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0075
Doc 3690

Monitoring | Statistics | DNS

This screen shows statistics for DNS (Domain Name System) activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with DNS servers, see the Configuration | System | Servers | DNS screen.

Figure 17-12 Monitoring / Statistics / DNS Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

.efresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests

The total number of DNS queries the VPN Concentrator made since it was last booted or reset. This number equals the sum of the numbers in the four cells below.

Responses

The number of DNS queries that were successfully resolved.

CORREIOS
0076
3690

Timeouts

The number of DNS queries that failed because there was no response from the server.

Server Unreachable

The number of DNS queries that failed because the address of the server is not reachable according to the VPN Concentrator's routing table.

Other Failures

The number of DNS queries that failed for an unspecified reason.

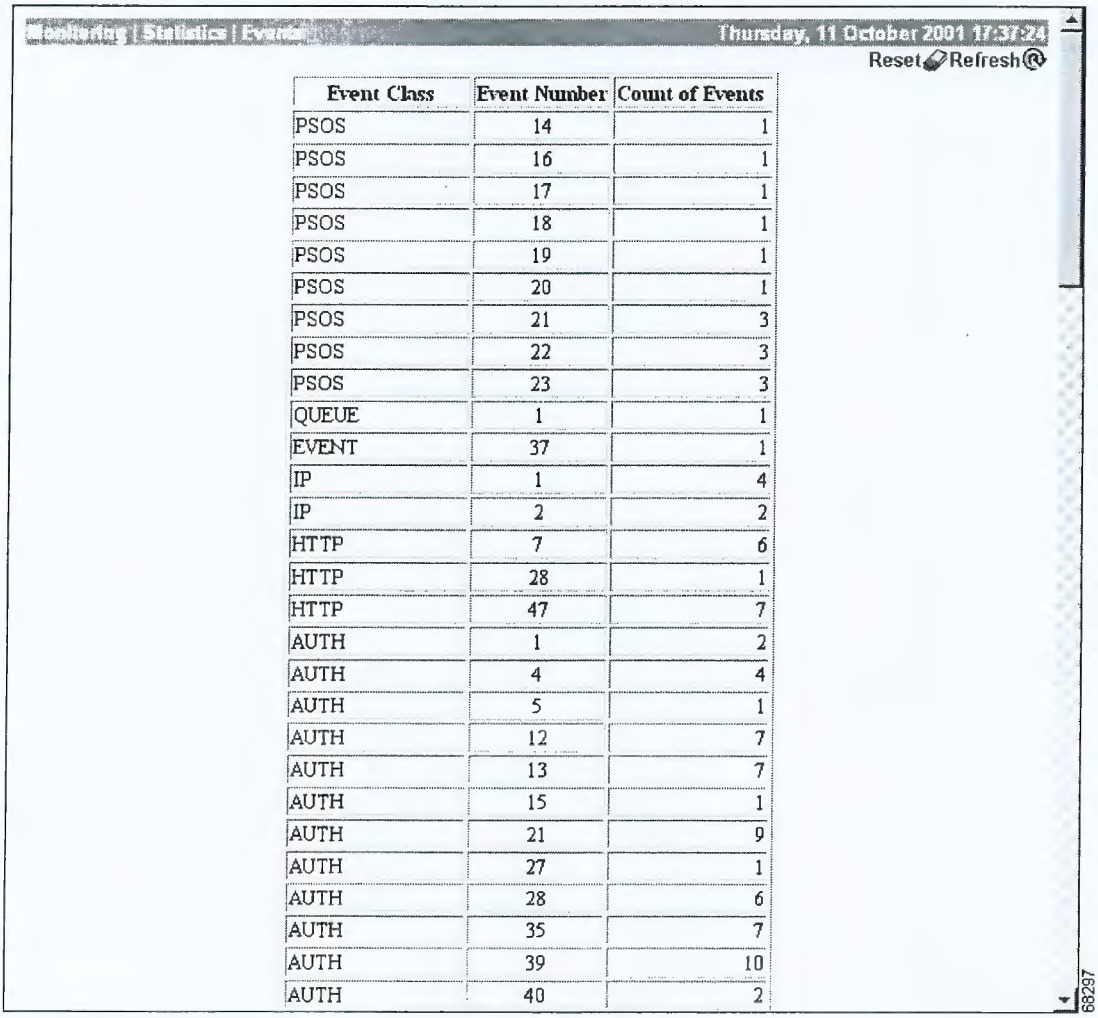
ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0077
Doc 3690

Monitoring | Statistics | Events

This screen shows statistics for all events on the VPN Concentrator since it was last booted or reset.

To configure event handling, see the Configuration | System | Events screens.

Figure 17-13 Monitoring | Statistics | Events Screen



Event Class	Event Number	Count of Events
PSOS	14	1
PSOS	16	1
PSOS	17	1
PSOS	18	1
PSOS	19	1
PSOS	20	1
PSOS	21	3
PSOS	22	3
PSOS	23	3
QUEUE	1	1
EVENT	37	1
IP	1	4
IP	2	2
HTTP	7	6
HTTP	28	1
HTTP	47	7
AUTH	1	2
AUTH	4	4
AUTH	5	1
AUTH	12	7
AUTH	13	7
AUTH	15	1
AUTH	21	9
AUTH	27	1
AUTH	28	6
AUTH	35	7
AUTH	39	10
AUTH	40	2

INPI Nº 03/2005 - CN
CPD - CORREIOS
Fls. Nº 0078
3690
Doc

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Event Class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator. For a description of event classes, see *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

Event Number

Event number is an Cisco-assigned reference number that denotes a specific event within the event class. For example, CONFIG event number 2 is "Reading configuration file." This reference number assists Cisco support personnel if they need to examine event statistics.

Count of Events

The number of times that specific event has occurred on the VPN Concentrator since it was last booted or reset.

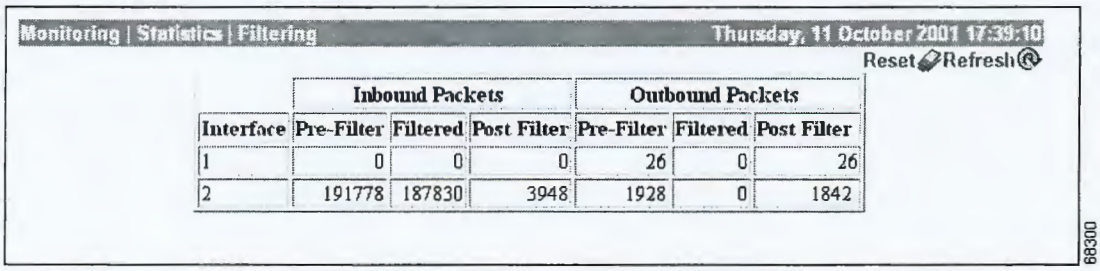
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0079
3690
Doc

Monitoring | Statistics | Filtering

This screen shows statistics for filtering of traffic that has passed through the interfaces on the VPN Concentrator since it was last booted or reset.

To configure filters, see the Configuration | Policy Management | Traffic Management screens. To apply filters to interfaces, see the Configuration | Interfaces screens. To apply filters to users and groups, see the Configuration | User Management screens.

Figure 17-14 Monitoring / Statistics / Filtering Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator network interface through which the filtered traffic has passed.

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.

0080
3690

Inbound Packets Pre-Filter

The total number of inbound packets received on this interface.

Inbound Packets Filtered

The number of inbound packets that have been filtered and dropped on this interface.

Inbound Packets Post Filter

The number of inbound packets that have been filtered and forwarded on this interface. This number equals Inbound Packets Pre-Filter minus Inbound Packets Filtered.

Outbound Packets Pre-Filter

The total number of outbound packets received on this interface.

Outbound Packets Filtered

The number of outbound packets that have been filtered and dropped on this interface.

Outbound Packets Post Filter

The number of outbound packets that have been filtered and forwarded on this interface. This number equals Outbound Packets Pre-Filter minus Outbound Packets Filtered.

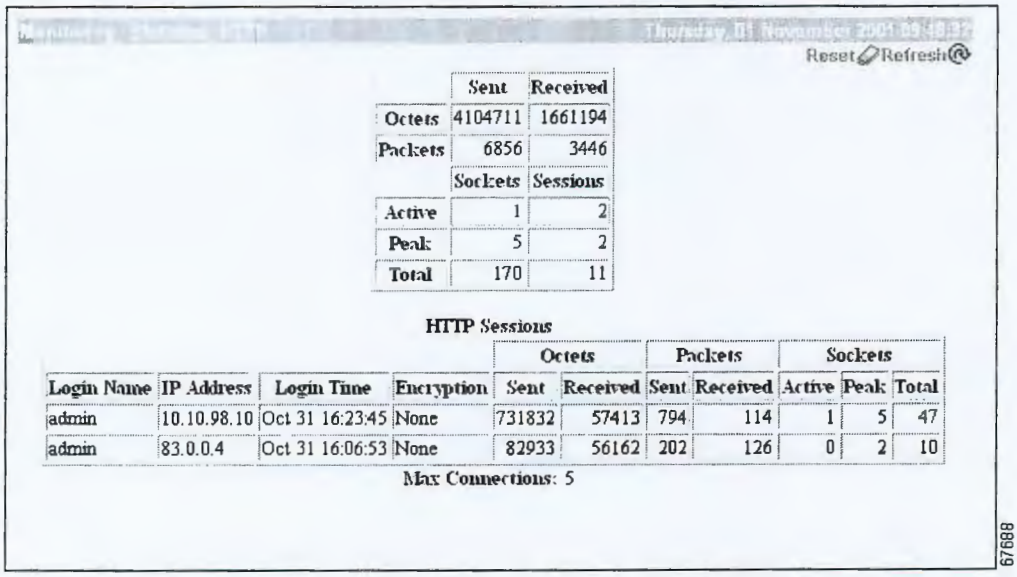
RQS nº 03/2005 - CN
CPMI - CORREIOS
0081
Fls Nº
3690
Doc

Monitoring | Statistics | HTTP

This screen shows statistics for HTTP activity on the VPN Concentrator since it was last booted or reset.

To configure system-wide HTTP server parameters, see the Configuration | System | Management Protocols | HTTP screen.

Figure 17-15 Monitoring | Statistics | HTTP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

CPMI - CORREIOS
Fls. Nº 0082
Doc 3690

Octets Sent/Received

The total number of HTTP octets (bytes) sent or received since the VPN Concentrator was last booted or reset.

Packets Sent/Received

The total number of HTTP packets sent or received since the VPN Concentrator was last booted or reset.

Packets Sent Sockets/Sessions

The number of HTTP sessions on the VPN Concentrator.

Active

The number of currently active HTTP connections on the VPN Concentrator.

Peak

The maximum number of HTTP connections that were simultaneously active on the VPN Concentrator since it was last booted or reset.

Total

The total number of HTTP connections on the VPN Concentrator since it was last booted or reset.

HTTP Sessions

This section provides information about HTTP sessions on the VPN Concentrator since it was last booted or reset.

Login Name

The name of the administrative user for the HTTP session.

IP Address

The IP address of the HTTP session.

Login Time

The time when the HTTP session began.

0083
Doc 3690

14.712

Encryption

The encryption method used in the HTTP session.

Octets Sent/Received

Number of octets sent or received during the HTTP session.

Packets Sent/Received

Number of packets sent or received during the HTTP session.

Sockets Active

The number of currently active sockets for the HTTP session.

Sockets Peak

The maximum number of sockets simultaneously active during the HTTP session.

Sockets Total

The total number of sockets active during the HTTP session.

Max Connections

The maximum number of concurrent HTTP connections for the VPN Concentrator since it was last rebooted or reset.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0084
Doc
3690

Monitoring | Statistics | IPSec

This screen shows statistics for IPSec activity—including current IPSec tunnels—on the VPN Concentrator since it was last booted or reset. These statistics conform to the IETF draft for the IPSec Flow Monitoring MIB.

The Monitoring | Sessions | Detail screens also show IPSec data.

To configure system-wide IPSec parameters and LAN-to-LAN connections, see the Configuration | System | Tunneling Protocols | IPSec screens. To configure IPSec parameters for users and groups, see Configuration | User Management. To configure IPSec parameters and SAs on rules in filters that govern data traffic, see Configuration | Policy Management | Traffic Management.

Figure 17-16 Monitoring | Statistics | IPSec Screen

Monitoring | Statistics | IPSec — Thursday, 11 October 2001 17:35:47

Reset Refresh

IKE (Phase 1) Statistics	
Active Tunnels	1
Total Tunnels	2
Received Bytes	61358
Sent Bytes	7980
Received Packets	775
Sent Packets	83
Received Packets Dropped	1
Sent Packets Dropped	0
Received Notifies	755
Sent Notifies	132
Received Phase-2 Exchanges	4
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	0
Phase-2 SA Delete Requests Sent	3
Initiated Tunnels	0
Failed Initiated Tunnels	0
Failed Remote Tunnels	0
Authentication Failures	0
Decryption Failures	0
Hash Validation Failures	0
System Capability Failures	0
No-SA Failures	0

IPSec (Phase 2) Statistics	
Active Tunnels	1
Total Tunnels	4
Received Bytes	6536
Sent Bytes	2104
Received Packets	44
Sent Packets	13
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	44
Failed Inbound Authentications	0
Outbound Authentications	13
Failed Outbound Authentications	0
Decryptions	44
Failed Decryptions	0
Encryptions	13
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

0085
3690

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IKE (Phase 1) Statistics

This table provides IPSec Phase 1 (IKE: Internet Key Exchange) global statistics. During IPSec Phase 1 (IKE), the two peers establish control tunnels through which they negotiate Security Associations.

Active Tunnels

The number of currently active IKE control tunnels, both for LAN-to-LAN connections and remote access.

Total Tunnels

The cumulative total of all currently and previously active IKE control tunnels, both for LAN-to-LAN connections and remote access.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IKE tunnels.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IKE tunnels.

Received Packets

The cumulative total of packets received by all currently and previously active IKE tunnels.

ROS nº 03/2005 - CN
CPI - CORREIOS
0086
Fls. Nº
3690
Doc.

Sent Packets

The cumulative total of packets sent by all currently and previously active IKE tunnels.

Received Packets Dropped

The cumulative total of packets that were dropped during receive processing by all currently and previously active IKE tunnels. If there is a problem with the content of a packet (such as hash failure, parsing error, or encryption failure) received in Phase 1 or the negotiation of Phase 2, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Sent Packets Dropped

The cumulative total of packets that were dropped during send processing by all currently and previously active IKE tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

eceived Notifies

The cumulative total of notify packets received by all currently and previously active IKE tunnels. A notify packet is an informational packet that is sent in response to a bad packet or to indicate status, for example: error packets, keepalive packets, etc.

Sent Notifies

The cumulative total of notify packets sent by all currently and previously active IKE tunnels. See comments for Received Notifies.

Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges received by all currently and previously active IKE tunnels, in other words, the total of Phase-2 negotiations received that were initiated by a remote peer. A complete exchange consists of three packets.

nt Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were sent by all currently and previously active and IKE tunnels, in other words, the total of Phase-2 negotiations initiated by this VPN Concentrator.

Invalid Phase-2 Exchanges Received

The cumulative total of IPSec Phase-2 exchanges that were received, found to be invalid because of protocol errors, and dropped, by all currently and previously active IKE tunnels. In other words, the total of Phase-2 negotiations that were initiated by a remote peer but that this VPN Concentrator dropped because of protocol errors.

ROS nº 0290/05 - CPMI - CORREIOS
Fls Nº 0087
Doc 3690

Invalid Phase-2 Exchanges Sent

The cumulative total of IPSec Phase-2 exchanges that were sent and were found to be invalid, by all currently and previously active IKE tunnels.

Rejected Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by a remote peer, received, and rejected by all currently and previously active IKE tunnels. Rejected exchanges indicate policy-related failures, such as configuration problems.

Rejected Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by this VPN Concentrator, sent, and rejected, by all currently and previously active IKE tunnels. See the previous comment.

Phase-2 SA Delete Requests Received

The cumulative total of requests to delete IPSec Phase-2 Security Associations received by all currently and previously active IKE tunnels.

Phase-2 SA Delete Requests Sent

The cumulative total of requests to delete IPSec Phase-2 Security Associations sent by all currently and previously active IKE tunnels.

Initiated Tunnels

The cumulative total of IKE tunnels that this VPN Concentrator initiated. The VPN Concentrator initiates tunnels only for LAN-to-LAN connections.

Failed Initiated Tunnels

The cumulative total of IKE tunnels that this VPN Concentrator initiated and that failed to activate.

Failed Remote Tunnels

The cumulative total of IKE tunnels that remote peers initiated and that failed to activate.

Authentication Failures

The cumulative total of authentication attempts that failed, by all currently and previously active IKE tunnels. Authentication failures indicate problems with preshared keys, digital certificates, or user-level authentication.

ECT 03/2005 - CN
CPMI - CORREIOS
0088
3690

Decryption Failures

The cumulative total of decryptions that failed, by all currently and previously active IKE tunnels. This number should be at or near zero; if not, check for misconfiguration or SEP module problems.

Hash Validation Failures

The cumulative total of hash validations that failed, by all currently and previously active IKE tunnels. Hash validation failures usually indicate misconfiguration or mismatched preshared keys or digital certificates.

System Capability Failures

The cumulative total of system capacity failures that occurred during processing of all currently and previously active IKE tunnels. These failures indicate that the system has run out of memory, or that the tunnel count exceeds the system maximum.

No-SA Failures

The cumulative total of nonexistent-Security Association failures that occurred during processing of all currently and previously active IKE tunnels. These failures occur when the system receives a packet for which it has no Security Association, and might indicate synchronization problems.

IPSec (Phase 2) Statistics

This table provides IPSec Phase 2 global statistics. During IPSec Phase 2, the two peers negotiate Security Associations that govern traffic within the tunnel.

Active Tunnels

The number of currently active IPSec Phase-2 tunnels, both for LAN-to-LAN connections and remote access.

Total Tunnels

The cumulative total of all currently and previously active IPSec Phase-2 tunnels, both for LAN-to-LAN connections and remote access.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IPSec Phase-2 tunnels, before decompression. In other words, total bytes of IPSec-only data received by the IPSec subsystem, before decompressing the IPSec payload.

0089
3690

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IPSec Phase-2 tunnels, after compression. In other words, total bytes of IPSec-only data sent by the IPSec subsystem, after compressing the IPSec payload.

Received Packets

The cumulative total of packets received by all currently and previously active IPSec Phase-2 tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IPSec Phase-2 tunnels.

Received Packets Dropped

The cumulative total of packets dropped during receive processing by all currently and previously active IPSec Phase-2 tunnels, excluding packets dropped due to anti-replay processing. If there is a problem with the content of a packet, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Received Packets Dropped (Anti-Replay)

The cumulative total of packets dropped during receive processing due to anti-replay errors, by all currently and previously active IPSec Phase-2 tunnels. If the sequence number of a packet is a duplicate or out of bounds, there might be a faulty network or a security breach, and the system drops the packet.

Sent Packets Dropped

The cumulative total of packets dropped during send processing by all currently and previously active IPSec Phase-2 tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Inbound Authentications

The cumulative total number of inbound individual packet authentications performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Inbound Authentications

The cumulative total of inbound packet authentications that failed, by all currently and previously active IPSec Phase-2 tunnels. Failed authentications could indicate corrupted packets or a potential security attack ("man in the middle").

Outbound Authentications

The cumulative total of outbound individual packet authentications performed by all currently and previously active IPSec Phase-2 tunnels.

0090
3690

14.705

Failed Outbound Authentications

The cumulative total of outbound packet authentications that failed, by all currently and previously active IPSec Phase-2 tunnels. This number should be zero or very small; if not, check the event log for an internal IPSec subsystem problem.

Decryptions

The cumulative total of inbound decryptions performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Decryptions

The cumulative total of inbound decryptions that failed, by all currently and previously active IPSec Phase-2 tunnels. This number should be zero or very small; if not, check for misconfiguration or SEP module problems.

ncryptions

The cumulative total of outbound encryptions performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Encryptions

The cumulative total of outbound encryptions that failed, by all currently and previously active IPSec Phase-2 tunnels. This number should be zero or very small; if not, check for IPSec subsystem or SEP module problems.

System Capability Failures

The total number of system capacity failures that occurred during processing of all currently and previously active IPSec Phase-2 tunnels. These failures indicate that the system has run out of memory or some other critical resource; check the event log.

-SA Failures

The cumulative total of nonexistent-Security Association failures which occurred during processing of all currently and previously active IPSec Phase-2 tunnels. These failures occur when the system receives an IPSec packet for which it has no Security Association, and might indicate synchronization problems.

Protocol Use Failures

The cumulative total of protocol use failures that occurred during processing of all currently and previously active IPSec Phase-2 tunnels. These failures indicate errors parsing IPSec packets.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0091
Doc 3690

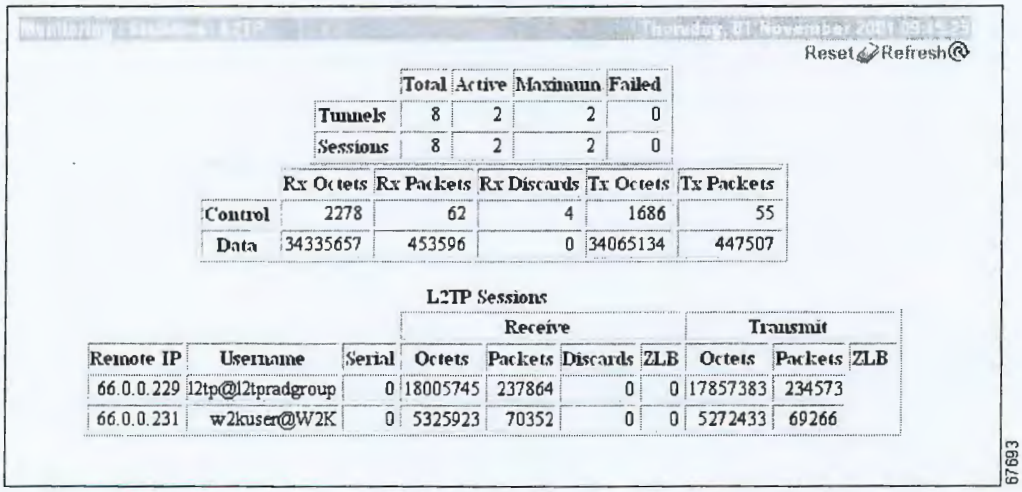
Monitoring | Statistics | L2TP

This screen shows statistics for L2TP activity on the VPN Concentrator since it was last booted or reset, and for current L2TP sessions.

The Monitoring | Sessions | Detail screens also show L2TP data.

To configure system-wide L2TP parameters, see the Configuration | System | Tunneling Protocols | L2TP screen. To configure L2TP parameters for users and groups, see Configuration | User Management. To configure L2TP on rules in filters that govern data traffic, see Configuration | Policy Management | Traffic Management.

Figure 17-17 Monitoring | Statistics | L2TP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

RDS nº 03/2005 - CN
File Nº 0092
Doc 3690

Total Tunnels

The total number of L2TP tunnels successfully established since the VPN Concentrator was last booted or reset.

Active Tunnels

The number of L2TP tunnels that are currently active.

Maximum Tunnels

The maximum number of L2TP tunnels that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Failed Tunnels

The number of L2TP tunnels that failed to become established since the VPN Concentrator was last booted or reset.

Total Sessions

The total number of user sessions successfully established through L2TP tunnels since the VPN Concentrator was last booted or reset.

Active Sessions

The number of user sessions that are currently active through PPTP tunnels. The L2TP Sessions table shows statistics for these sessions.

Maximum Sessions

The maximum number of user sessions that have been simultaneously active through L2TP tunnels on the VPN Concentrator since it was last booted or reset.

Failed Sessions

The number of sessions that failed to become established through L2TP tunnels since the VPN Concentrator was last booted or reset.

Rx Octets Control / Data

The number of L2TP control / data channel octets (bytes) received by the VPN Concentrator since it was last booted or reset.

CPMI - CORREIOS
0093
3690

Rx Packets Control / Data

The number of L2TP control / data channel packets received by the VPN Concentrator since it was last booted or reset.

Rx Discards Control / Data

The number of L2TP control / data channel packets received and discarded by the VPN Concentrator since it was last booted or reset.

Tx Octets Control / Data

The number of L2TP control/data channel octets (bytes) transmitted by the VPN Concentrator since it was last booted or reset.

Tx Packets Control / Data

The number of L2TP control/data channel packets transmitted by the VPN Concentrator since it was last booted or reset.

L2TP Sessions

This table shows statistics for active L2TP sessions on the VPN Concentrator. Each active session is a row.

Remote IP

The IP address of the remote host that established the L2TP tunnel for this session, in other words, the tunnel endpoint IP address. The Monitoring | Sessions screen shows the IP address assigned to the client using the tunnel.

Username

The username for the session within an L2TP tunnel. This is typically the login name of the remote user.

Serial

The serial number of the session within an L2TP tunnel. If there are multiple sessions using a tunnel, each session has a unique serial number.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0094
Doc. 3690

Receive Octets

The total number L2TP data octets (bytes) received by this session.

Receive Packets

The total number of L2TP data packets received by this session.

Receive Discards

The total number of L2TP data packets received and discarded by this session.

Receive ZLB

The total number of L2TP Zero Length Body acknowledgement data packets received by this session. ZLB packets are sent as acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Transmit Octets

The total number of L2TP data octets (bytes) transmitted by this session.

Transmit Packets

The total number of L2TP data packets transmitted by this session.

Transmit ZLB

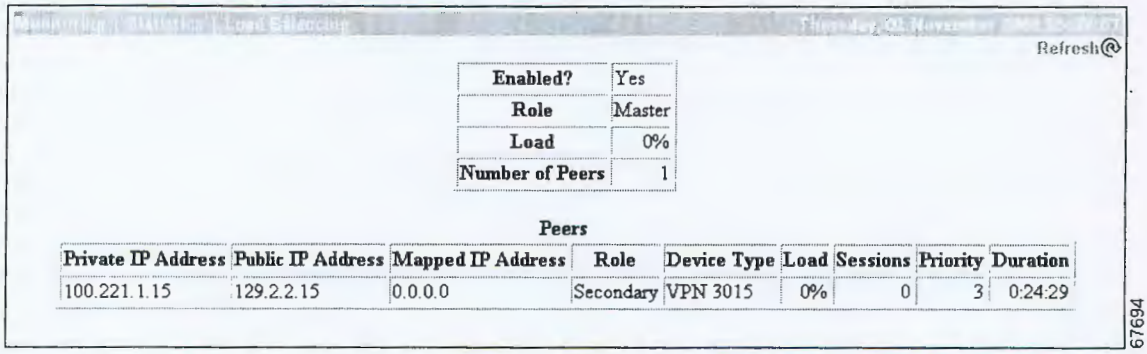
The total number of L2TP Zero Length Body acknowledgement packets transmitted by this session. ZLB packets are sent as acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

14.701
ROS nº 0095 - CN
CPMI - CORREIOS
Fls. Nº 0095
Doc. 3690

Monitoring | Statistics | Load Balancing

This screen shows statistics for load balancing on the VPN Concentrator since it was last booted or reset.

Figure 17-18 Monitoring | Statistics | Load Balancing Screen



Enabled?

Indicates whether load balancing has been enabled on this VPN Concentrator.

Role

The role of this VPN Concentrator within the virtual cluster. It is either a virtual cluster master or a secondary device.

Load

The percentage of the cluster's total session load that this VPN Concentrator is carrying.

Number of Peers

The number of other VPN Concentrators in the virtual cluster.

Peers

The peers chart shows configuration details and session statistics of the other VPN Concentrators in the virtual cluster.

Private IP Address

The private IP address of the peer.

ECT - CORREIOS
Fls. Nº 0096
3690
Doc

Public IP Address

The public IP address of the peer.

Mapped IP Address

The NAT address of the peer, if it has one.

Role

The role of the peer within the virtual cluster. It is either a virtual cluster master or a secondary device.

Device Type

The VPN Concentrator model (such as 3005 or 3015) of the peer.

Load

The percentage of the cluster's total session load that the peer is carrying. You can view this information only from the virtual cluster master device. If you are viewing this field from a secondary device, its value is N/A.

Sessions

The number of currently active sessions on the peer. You can view this information only from the virtual cluster master device. If you are viewing this field from a secondary device, its value is N/A.

Priority

The likelihood that this peer will become the master at power-up or if the current master fails. For more information on priorities, see the Configuration | System | Load Balancing section.

Duration

The length of time this device has been connected to the virtual cluster.

Refresh

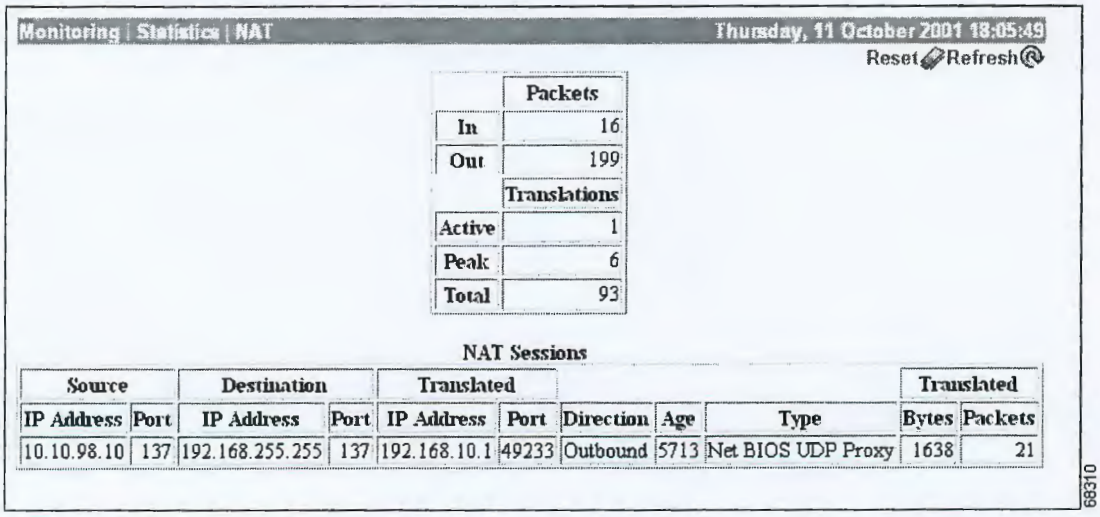
To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Nº 0097
3690

Monitoring | Statistics | NAT

This screen shows statistics for NAT (Network Address Translation) activity on the VPN Concentrator since it was last booted or reset.

Figure 17-19 Monitoring / Statistics / NAT screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Packets In/Out

The total of NAT packets inbound and outbound since the last time the VPN Concentrator was rebooted or reset.

0098
3690

Translations Active

The number of currently active NAT sessions.

Translations Peak

The maximum number of NAT sessions that were simultaneously active on the VPN Concentrator since it was last booted or reset.

Translations Total

The total number of NAT sessions on the VPN Concentrator since it was last booted or reset.

NAT Sessions

The following sections provide detailed information about active NAT sessions on the VPN Concentrator.

Source IP Address/Port

The source IP address and port for the NAT session.

Destination IP Address/Port

The destination IP address and port for the NAT session.

Translated IP Address/Port

The translated IP address and port for the NAT session. The VPN Concentrator uses this port number to keep track of which devices initiate data transfer; by keeping this record, the VPN Concentrator is able to correctly route responses.

Direction

The direction, inbound or outbound, of the data transferred for the NAT session.

Age

The number of half seconds remaining until the NAT session times out.

JU.696

Type

The type of packets for the NAT session. The possible types are:

- TCP NAT session
- UDP NAT session
- FTP session
- TFTP session
- NetBIOS over TCP Proxy
- NetBIOS over UDP Proxy
- NetBIOS Datagram Service

Translated Bytes/Packets

The total number of translated bytes and packets for the NAT session.

RQS nº 03/2005 - CN
CRMI - CORREIOS
0100
Fls: N
Doc 3690

Monitoring | Statistics | PPTP

This screen shows statistics for PPTP activity on the VPN Concentrator since it was last booted or reset, and for current PPTP sessions.

The Monitoring | Sessions | Detail screens also show PPTP data.

To configure system-wide PPTP parameters, see the Configuration | System | Tunneling Protocols | PPTP screen. To configure PPTP parameters for users and groups, see Configuration | User Management. To configure PPTP on rules in filters that govern data traffic, see Configuration | Policy Management | Traffic Management.

Figure 17-20 Monitoring | Statistics | PPTP Screen

Reset Refresh

	Total	Active	Maximum
Tunnels	1	1	1
Sessions	125	125	125

	Rx Octets	Rx Packets	Rx Discards	Tx Octets	Tx Packets
Control	103596	4445	0	74200	4195
Data	734949297	11950220	0	675427189	6727336

PPTP Sessions

		Receive				Transmit			ACK	
Peer IP	Username	Octets	Packets	Discards	ZLB	Octets	Packets	ZLB	Timeouts	Flow
66.0.0.130	user1	27553262	285944	0	48849	26487751	240445	3352	3352	None
66.0.0.130	user1	5891446	97068	0	46554	5399838	53509	2997	2997	None
66.0.0.130	user1	5891506	97084	0	46571	5404941	53943	3432	3432	None
66.0.0.130	user1	5891582	97088	0	46575	5404862	53935	3423	3423	None
66.0.0.130	user1	5891312	97068	0	46556	5401711	53675	3165	3165	None
66.0.0.130	user1	5891350	97071	0	46558	5398381	53396	2885	2885	None
66.0.0.130	user1	5891506	97081	0	46568	5402485	53738	3227	3227	None
66.0.0.130	user1	5891662	97096	0	46584	5400325	53559	3049	3049	None
66.0.0.130	user1	5891598	97092	0	46580	5401957	53695	3185	3185	None
66.0.0.130	user1	5891606	97091	0	46579	5404481	53906	3396	3396	None
66.0.0.130	user1	5891502	97082	0	46570	5399581	53497	2987	2987	None
66.0.0.130	user1	5891586	97090	0	46578	5401285	53639	3129	3129	None
66.0.0.130	user1	5891578	97088	0	46576	5400685	53589	3079	3079	None
66.0.0.130	user1	5891478	97079	0	46567	5401153	53628	3118	3118	None
66.0.0.130	user1	5891378	97073	0	46561	5404729	53926	3416	3416	None
66.0.0.130	user1	5891354	97071	0	46559	5404825	53934	3424	3424	None
66.0.0.130	user1	5891466	97081	0	46569	5404509	53908	3398	3398	None

67698

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

File N° 0101
Doc 3690

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Tunnels

The total number of PPTP tunnels created since the VPN Concentrator was last booted or reset, including those tunnels that failed to be established.

Active Tunnels

The number of PPTP tunnels that are currently active.

Maximum Tunnels

The maximum number of PPTP tunnels that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Total Sessions

The total number of user sessions through PPTP tunnels since the VPN Concentrator was last booted or reset.

Active Sessions

The number of user sessions that are currently active through PPTP tunnels. The PPTP Sessions table shows statistics for these sessions.

Maximum Sessions

The maximum number of user sessions that have been simultaneously active through PPTP tunnels on the VPN Concentrator since it was last booted or reset.

Rx Octets Control / Data

The number of PPTP control/data octets (bytes) received by the VPN Concentrator since it was last booted or reset.

ECT 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0102
Doc. 3690

Rx Packets Control / Data

The number of PPTP control/data packets received by the VPN Concentrator since it was last booted or reset.

Rx Discards Control / Data

The number of PPTP control/data packets received and discarded by the VPN Concentrator since it was last booted or reset.

Tx Octets Control / Data

The number of PPTP control/data octets (bytes) transmitted by the VPN Concentrator since it was last booted or reset.

Tx Packets Control / Data

The number of PPTP control/data packets transmitted by the VPN Concentrator since it was last booted or reset.

PPTP Sessions

This table shows statistics for active PPTP sessions on the VPN Concentrator. Each active session is a row.

Peer IP

The IP address of the peer host that established the PPTP tunnel for this session, in other words, the tunnel endpoint IP address. The Monitoring | Sessions screen shows the IP address assigned to the client using the tunnel.

Username

The username for the session within a PPTP tunnel. This is typically the login name of the remote user.

Receive Octets

The total number of PPTP data octets (bytes) received by this session.

Receive Packets

The total number of PPTP data packets received by this session.

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
Doc 3690

Receive Discards

The total number of PPTP data packets received and discarded by this session.

Receive ZLB

The total number of PPTP Zero Length Body acknowledgement data packets received by this session. ZLB packets are sent as GRE acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Transmit Octets

The total number of PPTP data octets (bytes) transmitted by this session.

Transmit Packets

The total number of PPTP data packets transmitted by this session.

Transmit ZLB

The total number of PPTP Zero Length Body acknowledgement packets transmitted by this session. ZLB packets are sent as GRE acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

ACK Timeouts

The total number of acknowledgement timeouts seen on PPTP data packets for this session. When the system times out waiting for a data packet on which to piggyback an acknowledgement, it sends a ZLB instead. Therefore, this number should equal the Transmit ZLB number.

Flow

The state of packet flow control for this PPTP session:

- Local = The local buffer is full. Packet flow for the local end of the session is OFF because the number of outstanding unacknowledged packets received from the peer is equal to the local window size.
- Peer = The peer buffer is full. Packet flow for the peer end of the session is OFF because the number of outstanding unacknowledged packets sent to the peer is equal to the peer's window size.
- Both = Both buffers are full. Packet flow for both ends of the session is OFF because the number of outstanding unacknowledged packets is equal to the window size on both ends.
- None = Neither end of the session has a full buffer. Packet flow for the session is ON. This is the normal operating state.

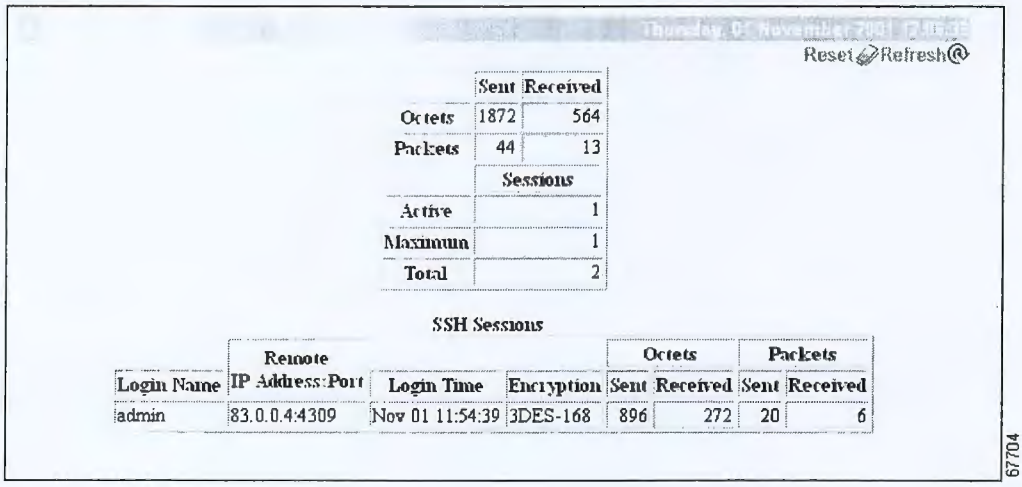
ECT nº 03/2003 - CN
CPMI - CORREIOS
Fls 0104
Doc 3690

Monitoring | Statistics | SSH

This screen shows statistics for SSH (Secure Shell) protocol traffic on the VPN Concentrator since it was last booted or reset.

To configure SSH, see Configuration | System | Management Protocols | SSH.

Figure 17-21 Monitoring | Statistics | SSH Screen



Octets Sent / Received

The total number of SSH octets (bytes) sent / received since the VPN Concentrator was last booted or reset.

Packets Sent / Received

The total number of SSH packets sent / received since the VPN Concentrator was last booted or reset.

Total Sessions

The total number of SSH sessions since the VPN Concentrator was last booted or reset.

Active Sessions

The number of currently active SSH sessions.

Max Sessions

The maximum number of simultaneously active SSH sessions on the VPN Concentrator.

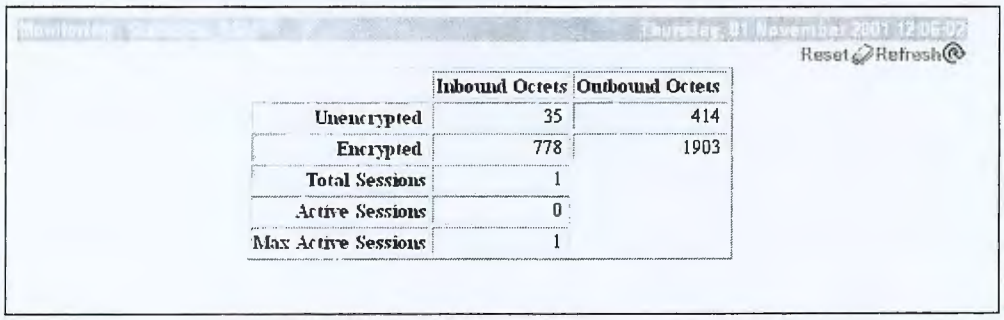
RQS nº 03/2005 - CN
CPMI - CORREIOS
0105
3690
Doc

Monitoring | Statistics | SSL

This screen shows statistics for SSL (Secure Sockets Layer) protocol traffic on the VPN Concentrator since it was last booted or reset.

To configure SSL, see Configuration | System | Management Protocols | SSL.

Figure 17-22 Monitoring / Statistics / SSL Screen



	Inbound Octets	Outbound Octets
Unencrypted	35	414
Encrypted	778	1903
Total Sessions	1	
Active Sessions	0	
Max Active Sessions	1	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Unencrypted Inbound Octets

The number of octets (bytes) of inbound traffic output by the decryption engine.

Encrypted Inbound Octets

The number of octets (bytes) of encrypted inbound traffic sent to the decryption engine. This number includes negotiation traffic.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0106
Doc 3690

Unencrypted Outbound Octets

The number of unencrypted outbound octets (bytes) sent to the encryption engine.

Encrypted Outbound Octets

The number of octets (bytes) of outbound traffic output by the encryption engine. This number includes negotiation traffic.

Total Sessions

The total number of SSL sessions.

Active Sessions

The number of currently active SSL sessions.

Max Active Sessions

The maximum number of SSL sessions simultaneously active at any one time.

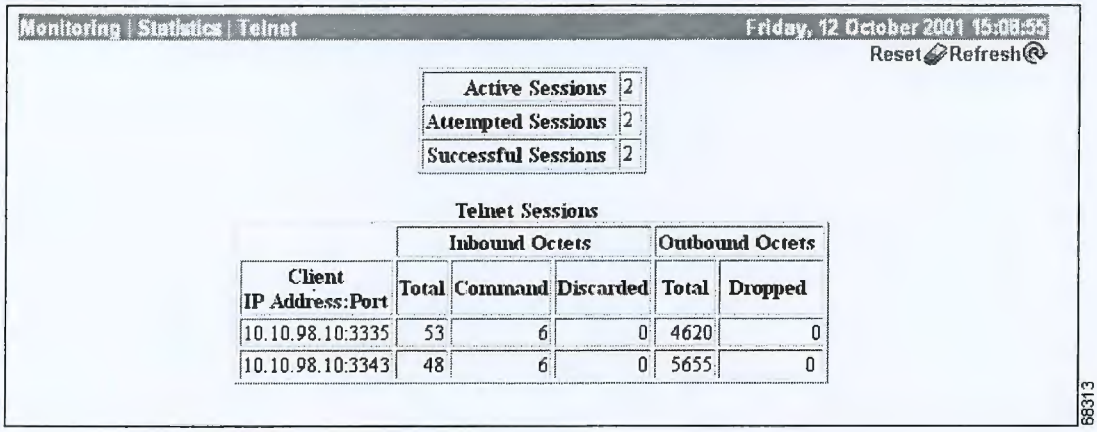
RQS nº 03/2005 - CN
CPMI CORREIOS
Fls Nº 0107
Doc 3690

Monitoring | Statistics | Telnet

This screen shows statistics for Telnet activity on the VPN Concentrator since it was last booted or reset, and for current Telnet sessions.

To configure the VPN Concentrator's Telnet server, see the Configuration | System | Management Protocols | Telnet screen.

Figure 17-23 Monitoring / Statistics / Telnet Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

0108
3690

Active Sessions

The number of active Telnet sessions. The Telnet Sessions table shows statistics for these sessions.

Attempted Sessions

The total number of attempts to establish Telnet sessions on the VPN Concentrator since it was last booted or reset.

Successful Sessions

The total number of Telnet sessions successfully established on the VPN Concentrator since it was last booted or reset.

Telnet Sessions

This table shows statistics for active Telnet sessions on the VPN Concentrator. Each active session is a row.

Client IP Address:Port

The IP address and TCP source port number of this session's remote Telnet client.

Inbound Octets Total

The total number of Telnet octets (bytes) received by this session.

Inbound Octets Command

The number of octets (bytes) containing Telnet commands or options, received by this session.

Inbound Octets Discarded

The number of Telnet octets (bytes) received and dropped during input processing by this session.

Outbound Octets Total

The total number of Telnet octets (bytes) transmitted by this session.

Outbound Octets Dropped

The number of outbound Telnet octets dropped during output processing by this session.

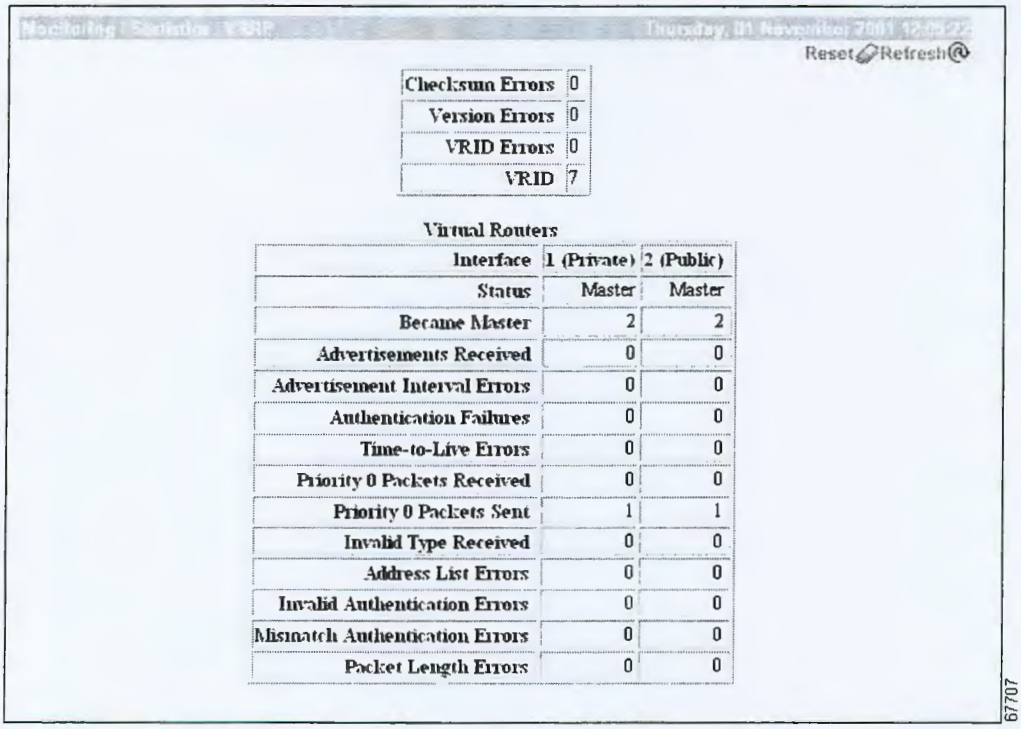
ROS nº 03/2008 - CN
CPMI - CORREIOS
Fls. nº 0109
3690

Monitoring | Statistics | VRRP

This screen shows status and statistics for VRRP (Virtual Router Redundancy Protocol) activity on the VPN Concentrator since it was last booted or reset.

To configure VRRP, see the Configuration | System | IP Routing | Redundancy screen.

Figure 17-24 Monitoring / Statistics / VRRP Screen



Checksum Errors	0
Version Errors	0
VRID Errors	0
VRID	7

Virtual Routers

Interface	1 (Private)	2 (Public)
Status	Master	Master
Became Master	2	2
Advertisements Received	0	0
Advertisement Interval Errors	0	0
Authentication Failures	0	0
Time-to-Live Errors	0	0
Priority 0 Packets Received	0	0
Priority 0 Packets Sent	1	1
Invalid Type Received	0	0
Address List Errors	0	0
Invalid Authentication Errors	0	0
Mismatch Authentication Errors	0	0
Packet Length Errors	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

14.686
ROS nº 03/2005 - CN
CPMI - CORREIOS
0110
3690

Checksum Errors

The total number of VRRP packets received with an invalid VRRP checksum value.

Version Errors

The total number of VRRP packets received with an unknown or unsupported version number. The VPN Concentrator supports VRRP version 2 as defined in RFC 2338.

VRID Errors

The total number of VRRP packets received with an invalid VRRP Group ID number.

VRID

The identification number that uniquely identifies the group of virtual routers to which this VPN Concentrator belongs.

- Not Configured = VRRP has not been configured or enabled.

Virtual Routers

This table shows statistics for the virtual router on each configured VRRP interface on this VPN Concentrator.

Interface: 1 (Private), 2 (Public), 3 (External)

The Ethernet interface configured for VRRP.

Status

The status of the VRRP router in this VPN Concentrator:

- Master = VRRP is enabled and the router is functioning as the Master router.
- Backup = VRRP is enabled and the router is functioning as a Backup router, monitoring the status of the Master router.
- Init = VRRP has been configured but is disabled. The router is waiting to be enabled (initialized).

Became Master

The total number of times that this VPN Concentrator has become a VRRP Master router after having a different role. This number should be the same in all columns.

Advertisements Received

The total number of VRRP advertisements received by this interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0111
Fls. Nº
Doc 3690

Advertisement Interval Errors

The total number of VRRP advertisement packets received by this interface, in which the advertisement interval differs from the interval configured on this VPN Concentrator.

Authentication Failures

The total number of VRRP packets received by this interface that do not pass the authentication check.

Time-to-Live Errors

The total number of VRRP packets received by this interface with IP TTL (Time-To-Live) not equal to 255. All VRRP packets must have TTL = 255.

Priority 0 Packets Received

The total number of VRRP packets received by this interface with a priority of 0. Priority 0 packets indicate that the current Master router has stopped participating in VRRP.

Priority 0 Packets Sent

The total number of VRRP packets sent by this interface with a priority of 0. Priority 0 packets indicate that the current Master router has stopped participating in VRRP.

Invalid Type Received

The number of VRRP packets received by this interface with an invalid value in the Type field. For VRRP version 2, the only valid Type value is 1, which indicates an advertisement packet.

Address List Errors

The total number of packets received for which the address list does not match the list configured on this VPN Concentrator.

Invalid Authentication Errors

The total number of packets received by this interface with an unknown authentication type.

Mismatch Authentication Errors

The total number of packets received by this interface with an authentication type that differs from the configured authentication type.

Packet Length Errors

The total number of packets received by this interface with a packet length less than the length of the VRRP header.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0112
3690

Monitoring | Statistics | MIB-II

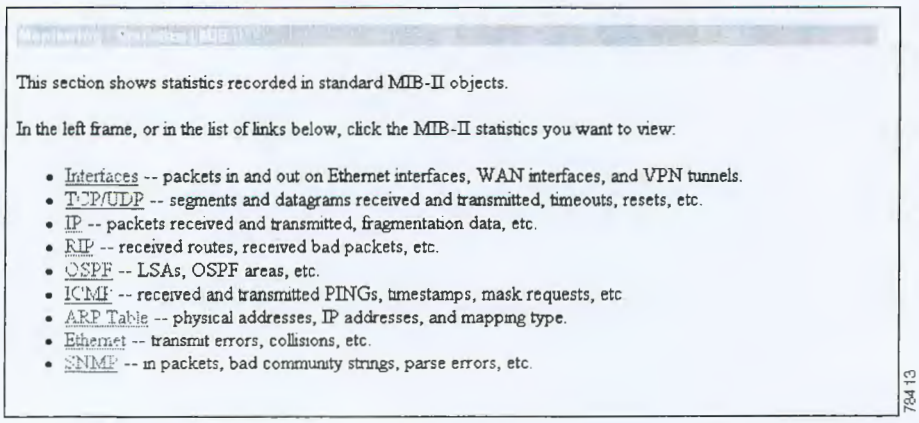
This section of the Manager lets you view statistics that are recorded in standard MIB-II objects on the VPN Concentrator. MIB-II (Management Information Base, version 2) objects are variables that contain data about the system. They are defined as part of the Simple Network Management Protocol (SNMP); and SNMP-based network management systems can query the VPN Concentrator to gather the data.

Each subsequent screen displays the data for a standard MIB-II group of objects:

- Interfaces: packets sent and received on network interfaces and VPN tunnels.
- TCP/UDP: Transmission Control Protocol and User Datagram Protocol segments and datagrams sent and received, etc.
- IP: Internet Protocol packets sent and received, fragmentation and reassembly data, etc.
- RIP: Routing Information Protocol global route changes, bad packets and bad routes received, etc.
- OSPF: Open Shortest Path First protocol LSA data, Area data, etc.
- ICMP: Internet Control Message Protocol ping, timestamp, and address mask requests and replies, etc.
- ARP Table: Address Resolution Protocol physical (MAC) addresses, IP addresses, and mapping types.
- Ethernet: errors and collisions, MAC errors, etc.
- SNMP: Simple Network Management Protocol requests, bad community strings, parsing errors, etc.

To configure and enable the VPN Concentrator's SNMP server, see the Configuration | System | Management Protocols | SNMP screen.

Figure 17-25 Monitoring / Statistics / MIB-II Screen

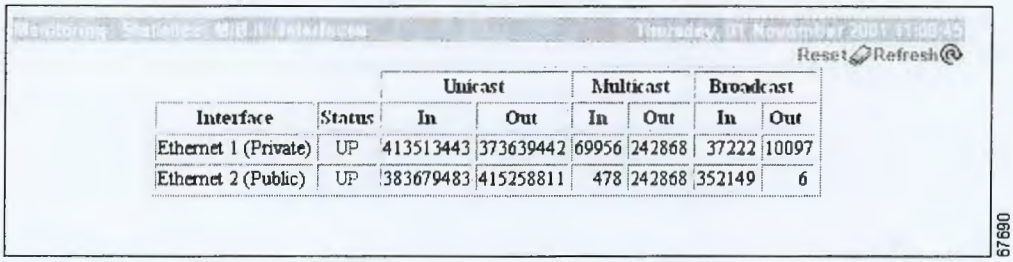


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0113
3690

Monitoring | Statistics | MIB-II | Interfaces

This screen shows statistics in MIB-II objects for VPN Concentrator interfaces since the system was last booted or reset. This screen also shows statistics for VPN tunnels as logical interfaces. RFC 2233 defines interface MIB objects.

Figure 17-26 Monitoring | Statistics | MIB-II | Interfaces Screen



		Unicast		Multicast		Broadcast	
Interface	Status	In	Out	In	Out	In	Out
Ethernet 1 (Private)	UP	413513443	373639442	69956	242868	37222	10097
Ethernet 2 (Public)	UP	383679483	415258811	478	242868	352149	6

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator interface:

- Ethernet 1 (Private) = Ethernet 1 (Private) interface.
- Ethernet 2 (Public) = Ethernet 2 (Public) interface.
- Ethernet 3 (External) = Ethernet 3 (External) interface.
- 1000 and up = VPN tunnels, which are treated as logical interfaces.

0114
3690

J4.681
J

Status

The operational status of this interface:

- UP = configured and enabled, ready to pass data traffic.
- DOWN = configured but disabled.
- Testing = in test mode; no regular data traffic can pass.
- Dormant = configured and enabled but waiting for an external action, such as an incoming connection.
- Not Present = missing hardware components.
- Lower Layer Down = not operational because a lower-layer interface is down.
- Unknown = not configured.

Unicast In

The number of unicast packets that were received by this interface. Unicast packets are those addressed to a single host.

Unicast Out

The number of unicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Multicast In

The number of multicast packets that were received by this interface. Multicast packets are those addressed to a specific group of hosts.

Multicast Out

The number of multicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Broadcast In

The number of broadcast packets that were received by this interface. Broadcast packets are those addressed to all hosts on a network.

Broadcast Out

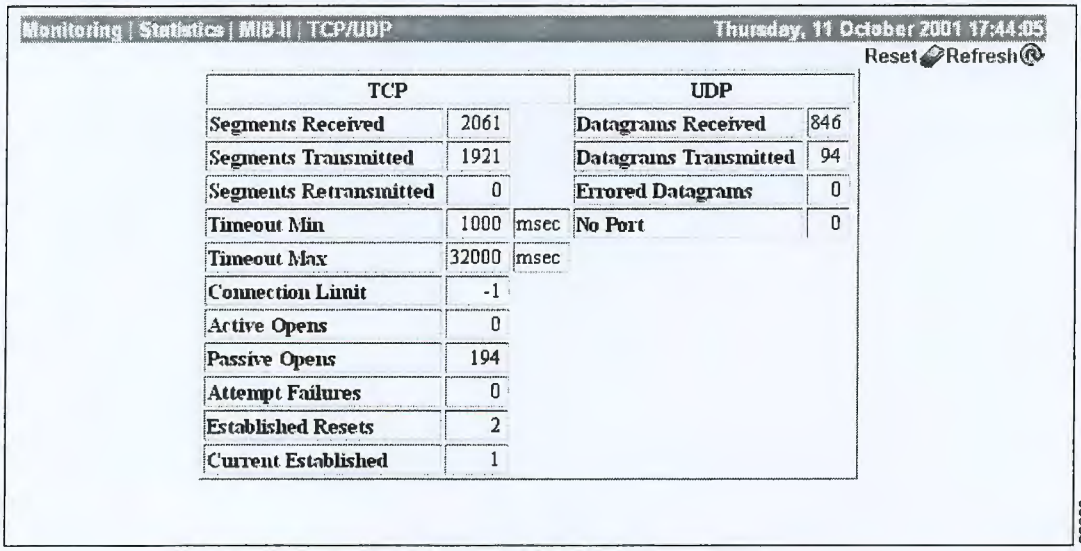
The number of broadcast packets that were routed to this interface for transmission, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

ECT CORREIOS
0115
3690
Doc

Monitoring | Statistics | MIB-II | TCP/UDP

This screen shows statistics in MIB-II objects for TCP and UDP traffic on the VPN Concentrator since it was last booted or reset. RFC 2012 defines TCP MIB objects, and RFC 2013 defines UDP MIB objects.

Figure 17-27 Monitoring | Statistics | MIB-II | TCP/UDP Screen



TCP			UDP	
Segments Received	2061		Datagrams Received	846
Segments Transmitted	1921		Datagrams Transmitted	94
Segments Retransmitted	0		Errored Datagrams	0
Timeout Min	1000	msec	No Port	0
Timeout Max	32000	msec		
Connection Limit	-1			
Active Opens	0			
Passive Opens	194			
Attempt Failures	0			
Established Resets	2			
Current Established	1			

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

TCP Segments Received

The total number of segments received, including those received in error and those received on currently established connections. Segment is the official TCP name for what is often called a data packet.

14,679

TCP Segments Transmitted

The total number of segments sent, including those on currently established connections but excluding those containing only retransmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Retransmitted

The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Timeout Min

The minimum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Timeout Max

The maximum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Connection Limit

The limit on the total number of TCP connections that the system can support. A value of -1 means there is no limit.

TCP Active Opens

The number of TCP connections that went directly from an unconnected state to a connection-synchronizing state, bypassing the listening state. These connections are allowed, but they are usually in the minority.

TCP Passive Opens

The number of TCP connections that went from a listening state to a connection-synchronizing state. These connections are usually in the majority.

TCP Attempt Failures

The number of TCP connection attempts that failed. Technically this is the number of TCP connections that went to an unconnected state, plus the number that went to a listening state, from a connection-synchronizing state.

0117
Doc 3690

TCP Established Resets

The number of established TCP connections that abruptly closed, bypassing graceful termination.

TCP Current Established

The number of TCP connections that are currently established or are gracefully terminating.

UDP Datagrams Received

The total number of UDP datagrams received. Datagram is the official UDP name for what is casually called a data packet.

UDP Datagrams Transmitted

The total number of UDP datagrams sent. Datagram is the official UDP name for what is casually called a data packet.

UDP Errored Datagrams

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port (UDP No Port). Datagram is the official UDP name for what is casually called a data packet.

UDP No Port

The total number of received UDP datagrams that could not be delivered because there was no application at the destination port. Datagram is the official UDP name for what is casually called a data packet.

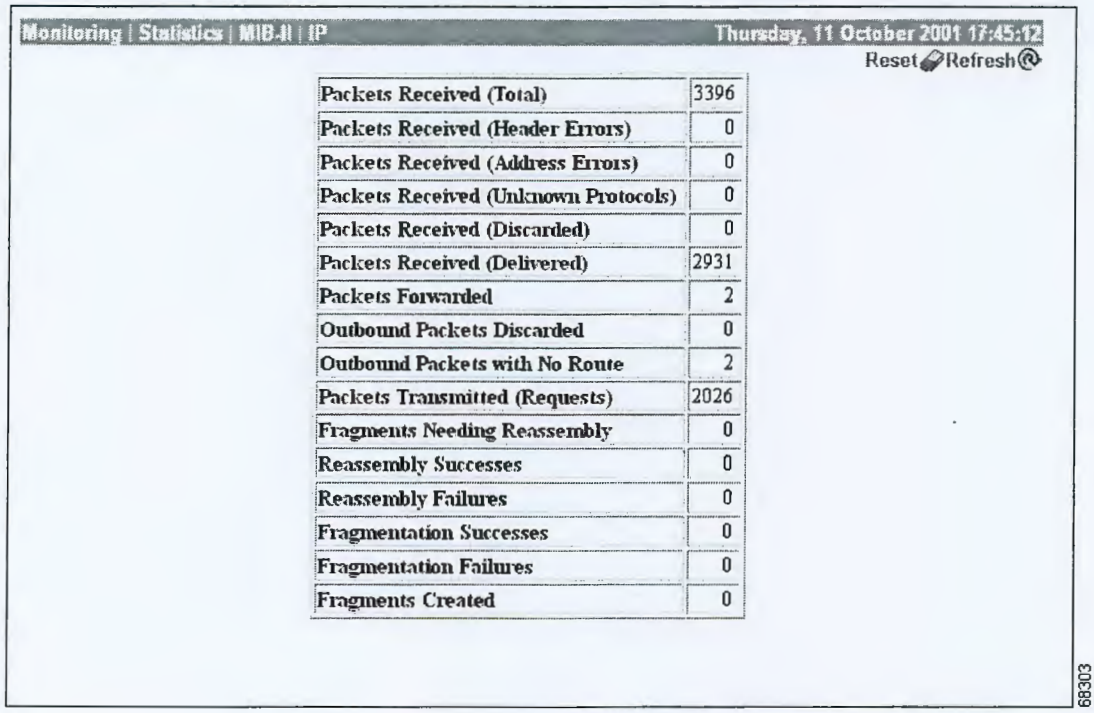
Go to top of help page.

0118
3690

Monitoring | Statistics | MIB-II | IP

This screen shows statistics in MIB-II objects for IP traffic on the VPN Concentrator since it was last booted or reset. RFC 2011 defines IP MIB objects.

Figure 17-28 Monitoring | Statistics | MIB-II | IP Screen



Packets Received (Total)	3396
Packets Received (Header Errors)	0
Packets Received (Address Errors)	0
Packets Received (Unknown Protocols)	0
Packets Received (Discarded)	0
Packets Received (Delivered)	2931
Packets Forwarded	2
Outbound Packets Discarded	0
Outbound Packets with No Route	2
Packets Transmitted (Requests)	2026
Fragments Needing Reassembly	0
Reassembly Successes	0
Reassembly Failures	0
Fragmentation Successes	0
Fragmentation Failures	0
Fragments Created	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0119
Doc 3690

Packets Received (Total)

The total number of IP data packets received by the VPN Concentrator, including those received with errors.

Packets Received (Header Errors)

The number of IP data packets received and discarded due to errors in IP headers, including bad check sums, version number mismatches, other format errors, etc.

Packets Received (Address Errors)

The number of IP data packets received and discarded because the IP address in the destination field was not a valid address for the VPN Concentrator. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E).

Packets Received (Unknown Protocols)

The number of IP data packets received and discarded because of an unknown or unsupported protocol.

Packets Received (Discarded)

The number of IP data packets received that had no problems preventing continued processing, but that were discarded (for example, for lack of buffer space). This number does not include any packets discarded while awaiting reassembly.

Packets Received (Delivered)

The number of IP data packets received and successfully delivered to IP user protocols (including ICMP) on the VPN Concentrator; i.e., the VPN Concentrator was the final destination.

Packets Forwarded

The number of IP data packets received and forwarded to destinations other than the VPN Concentrator.

Outbound Packets Discarded

The number of outbound IP data packets that had no problems preventing their transmission to a destination, but that were discarded (for example, for lack of buffer space).

CPMI – CORREIOS
Fls. 0120
3690

Outbound Packets with No Route

The number of outbound IP data packets discarded because no route could be found to transmit them to their destination. This number includes any packets that the VPN Concentrator could not route because all of its default routers are down.

Packets Transmitted (Requests)

The number of IP data packets that local IP user protocols (including ICMP) supplied to transmission requests. This number does not include any packets counted in Packets Forwarded.

Fragments Needing Reassembly

The number of IP fragments received by the VPN Concentrator that needed to be reassembled.

Reassembly Successes

The number of IP data packets successfully reassembled.

Reassembly Failures

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). This number is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.

Fragmentation Successes

The number of IP data packets that have been successfully fragmented by the VPN Concentrator.

Fragmentation Failures

The number of IP data packets that have been discarded because they needed to be fragmented but could not be fragmented (for example, because the Don't Fragment flag was set).

Fragments Created

The number of IP data packet fragments that have been generated by the VPN Concentrator.

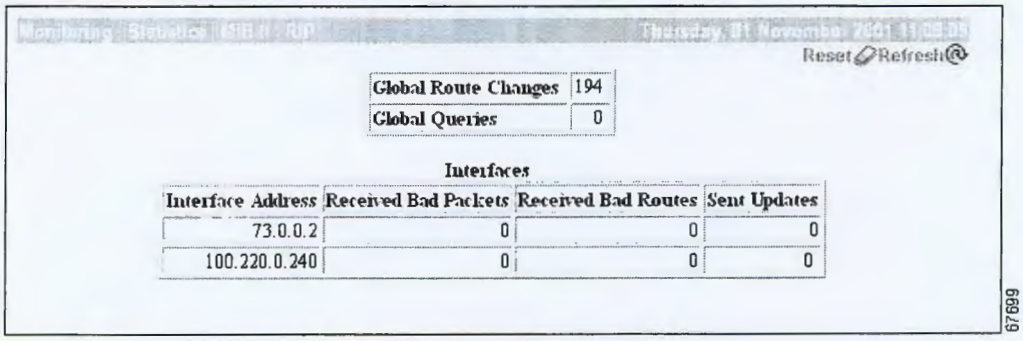
0121
3690

Monitoring | Statistics | MIB-II | RIP

This screen shows statistics in MIB-II objects for RIP version 2 traffic on the VPN Concentrator since it was last booted or reset. RFC 1724 defines RIP version 2 MIB objects.

To configure RIP on interfaces, see Configuration | Interfaces.

Figure 17-29 Monitoring / Statistics / MIB-II / RIP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Global Route Changes

The total number of route changes made to the IP route database by RIP. This number does not include changes that only refresh the age route of a route.

Global Queries

The total number of responses sent to RIP queries from other systems.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0122
Doc: 3690

14.675

Interfaces

This table shows a row of statistics for each configured interface.

Interface Address

The IP address configured on the interface.

Received Bad Packets

The number of RIP response packets received by this interface that were subsequently discarded for any reason (such as wrong version or unknown command type).

Received Bad Routes

The number of routes in valid RIP packets received by this interface that were ignored for any reason (such as unknown address family or invalid metric).

Sent Updates

The number of triggered RIP updates actually sent by this interface. This number does not include full updates sent containing new information.

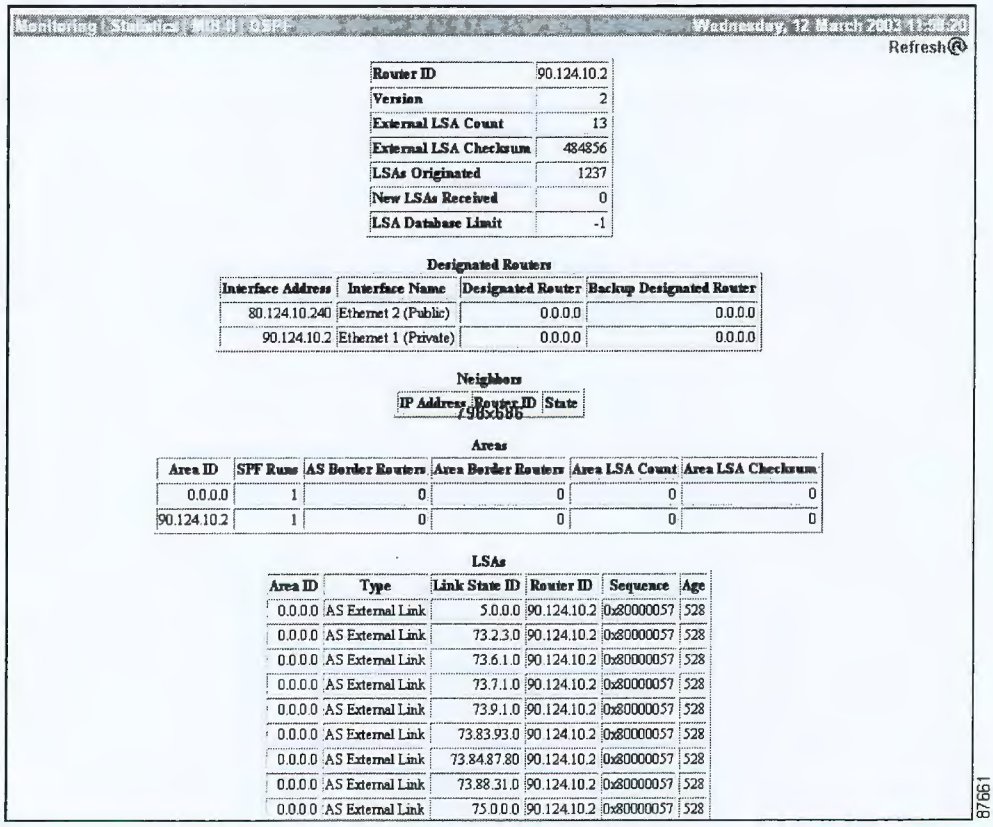
ROS - 03/2005 - CN
CPMI 0123
Fls N°
Doc 3690

Monitoring | Statistics | MIB-II | OSPF

This screen shows statistics in MIB-II objects for OSPF version 2 traffic on the VPN Concentrator since it was last booted or reset. RFC 1850a defines OSPF version 2 MIB objects.

To configure OSPF on interfaces, see Configuration | Interfaces. To configure system-wide OSPF parameters, see Configuration | System | IP Routing.

Figure 17-30 Monitoring / Statistics / MIB-II / OSPF Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Router ID

The VPN Concentrator OSPF router ID. This ID uniquely identifies the VPN Concentrator to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network. 0.0.0.0 means no router is configured.

Version

The current version number of the OSPF protocol running on the VPN Concentrator.

External LSA Count

The number of external Link-State Advertisements (LSAs) in the link-state database. LSAs from neighboring OSPF Autonomous Systems (AS) describe the state of the AS router's interfaces and routing paths.

External LSA Checksum

The sum of the check sums of the external Link-State Advertisements in the link-state database. You can use this sum to determine if there has been a change in the OSPF router link-state database of the system, and to compare its database with other routers.

LSAs Originated

The number of new Link-State Advertisements that the system has originated. This number increments each time the OSPF router originates a new LSA.

New LSAs Received

The number of Link-State Advertisements received that are completely new LSAs. This number does not include newer instances of self-originated LSAs.

LSA Database Limit

The maximum number of external LSAs that can be stored in the link-state database. A value of -1 means there is no limit.

Designated Routers

This table shows a row of statistics for each enabled VPN Concentrator interface. When OSPF routing is enabled on an interface, that interface communicates with other OSPF routers in its area, and each area elects one OSPF router to be the Designated Router.

Interface Address

The IP address of the VPN Concentrator interface that communicates with its area.

0125
3690

Interface Name

The VPN Concentrator interface that communicates with its area:

- Ethernet 1 (Private) = Ethernet 1 (Private) interface.
- Ethernet 2 (Public) = Ethernet 2 (Public) interface.
- Ethernet 3 (External) = Ethernet 3 (External) interface.

Designated Router

The IP address of the Designated Router in this OSPF area.

Backup Designated Router

The IP address of the backup Designated Router in this OSPF area.

Neighbors

This table shows a row of statistics for each OSPF neighbor, for all areas in which the VPN Concentrator participates. A neighbor is another OSPF router in an OSPF area, and this table includes all such areas for the VPN Concentrator.

IP Address

The IP address of the neighboring OSPF router.

Router ID

The router ID of the neighboring OSPF router, which uniquely identifies it to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier. By convention, however, it is the same as the IP address of the interface that is connected to the OSPF router network.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0126
3690

14.669

State

The state of the relationship with this neighboring OSPF router:

- Down = (Red) The VPN Concentrator has received no recent information from this neighbor. The neighbor might be out of service, or it might not have been in service long enough to establish its presence (at startup).
- Initializing = The VPN Concentrator has received a Hello packet from this neighbor, but it has not yet established bidirectional communication.
- Attempting = This state applies only to neighbors in an NBMA (Non-Broadcast Multi-Access) OSPF network. It indicates that the VPN Concentrator has received no recent information from this neighbor, but it is trying to establish contact by sending Hello packets at the Hello Interval.
- Two Way = The VPN Concentrator has established bidirectional communication with this neighbor, but has not established adjacency, in other words, they are not exchanging routing information.
- Exchange Start = The VPN Concentrator and this neighbor are in the first step of establishing an adjacency relationship.
- Exchanging = The VPN Concentrator is describing its entire link state database by sending Database Description packets to this neighbor, to establish an adjacency relationship.
- Loading = The VPN Concentrator is sending Link State Request packets to this neighbor asking for the more recent LSAs that have been discovered but not yet received in the Exchange state.
- Full = (Green) The VPN Concentrator is in a fully adjacent relationship with this neighbor. This adjacency now appears in router LSAs and network LSAs.

Areas

This table shows a row of statistics for each OSPF Area.

Area ID

The Area ID identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. 0.0.0.0 identifies a special area—the backbone—that contains all area border routers.

F Runs

The number of times that the system has calculated the intra-area route table (SPF, or Shortest Path First table) using the link-state database of this area.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0127
Doc 3690

AS Border Routers

The total number of Autonomous System border routers reachable within this area.

Area Border Routers

The total number of area border routers reachable within this area.

Area LSA Count

The total number of Link-State Advertisements in the link-state database of this area, excluding AS external LSAs.

Area LSA Checksum

The sum of the check sums of the Link-State Advertisements in the link-state database of this area. This sum excludes external LSAs. You can use this sum to determine if there has been a change in the link-state database of the area, and to compare its database with other routers.

External LSAs

This table shows a row for each external Link-State Advertisement in the link-state database.

Area ID

The Area ID identifies the Area from which the LSA was received.

Type

The LSA type. Each LSA type has a different format:

- Router Link = Describes the states of the router's interfaces (LS Type 1).
- Network Link = Describes the set of routers attached to the network (LS Type 2).
- Summary Link = Describes routes to networks (LS Type 3).
- AS Summary Link = Describes routes to AS boundary routers (LS Type 4).
- AS External Link = Describes routes to destinations external to the AS (LS Type 5).
- Multicast Link = Describes group membership for multicast OSPF routing (LS Type 6).
- NSSA External Link = Describes routing for NSSAs: Not-So-Stubby-Areas (LS Type 7).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0128
Doc 3690

Link State ID

Either a router ID or an IP address that identifies the piece of the routing domain being described by the LSA.

Router ID

The identifier of the router in the Autonomous System that originated this LSA.

Sequence

The sequence number of this LSA. Sequence numbers are linear. They are used to detect old and duplicate LSAs. The larger the number, the more recent the LSA.

Age

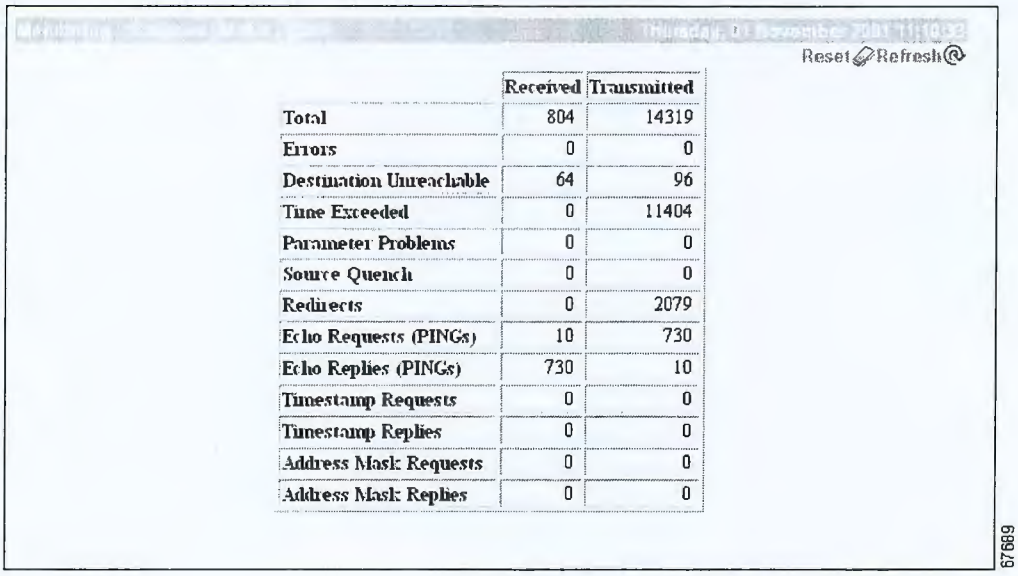
The age of the LSA in seconds.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0129
3690

Monitoring | Statistics | MIB-II | ICMP

This screen shows statistics in MIB-II objects for ICMP traffic on the VPN Concentrator since it was last booted or reset. RFC 2011 defines ICMP MIB objects.

Figure 17-31 Monitoring | Statistics | MIB-II | ICMP Screen



	Received	Transmitted
Total	804	14319
Errors	0	0
Destination Unreachable	64	96
Time Exceeded	0	11404
Parameter Problems	0	0
Source Quench	0	0
Redirects	0	2079
Echo Requests (PINGs)	10	730
Echo Replies (PINGs)	730	10
Timestamp Requests	0	0
Timestamp Replies	0	0
Address Mask Requests	0	0
Address Mask Replies	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

ROS nº 03/2005 - CN
Fls 0130
Doc 3690

Total Received / Transmitted

The total number of ICMP messages that the VPN Concentrator received / sent. This number includes messages counted as Errors Received / Transmitted. ICMP messages solicit and provide information about the network environment.

Errors Received / Transmitted

The number of ICMP messages that the VPN Concentrator received but determined to have ICMP-specific errors (bad ICMP check sums, bad length, etc.).

The number of ICMP messages that the VPN Concentrator did not send due to problems within ICMP such as a lack of buffers.

Destination Unreachable Received / Transmitted

The number of ICMP Destination Unreachable messages received / sent. Destination Unreachable messages apply to many network situations, including inability to determine a route, an unusable source route specified, and the Don't Fragment flag set for a packet that must be fragmented.

Time Exceeded Received / Transmitted

The number of ICMP Time Exceeded messages received / sent. Time Exceeded messages indicate that the lifetime of the packet has expired, or that a router cannot reassemble a packet within a time limit.

Parameter Problems Received / Transmitted

The number of ICMP Parameter Problem messages received / sent. Parameter Problem messages indicate a syntactic or semantic error in an IP header.

Source Quench Received / Transmitted

The number of ICMP Source Quench messages received / sent. Source Quench messages provide rudimentary flow control; they request a reduction in the rate of sending traffic on the network.

Redirects Received / Transmitted

The number of ICMP Redirect messages received / sent. Redirect messages advise that there is a better route to a particular destination.

0131
3690

Echo Requests (PINGs) Received / Transmitted

The number of ICMP Echo (request) messages received / sent. Echo messages are probably the most visible ICMP messages. They test the communication path between network entities by asking for Echo Reply response messages.

Echo Replies (PINGs) Received / Transmitted

The number of ICMP Echo Reply messages received / sent. Echo Reply messages are sent in response to Echo messages, to test the communication path between network entities.

Timestamp Requests Received / Transmitted

The number of ICMP Timestamp (request) messages received / sent. Timestamp messages measure the propagation delay between network entities by including the originating time in the message, and asking for the receipt time in a Timestamp Reply message.

Timestamp Replies Received / Transmitted

The number of ICMP Timestamp Reply messages received / sent. Timestamp Reply messages are sent in response to Timestamp messages, to measure propagation delay in the network.

Address Mask Requests Received / Transmitted

The number of ICMP Address Mask Request messages received / sent. Address Mask Request messages ask for the address (subnet) mask for the LAN to which a router connects.

Address Mask Replies Received / Transmitted

The number of ICMP Address Mask Reply messages received / sent. Address Mask Reply messages respond to Address Mask Request messages by supplying the address (subnet) mask for the LAN to which a router connects.

14.664
ROS nº 02/2005 - CN
CPMI - CORREIOS
Fls. Nº 0132
Doc 3690

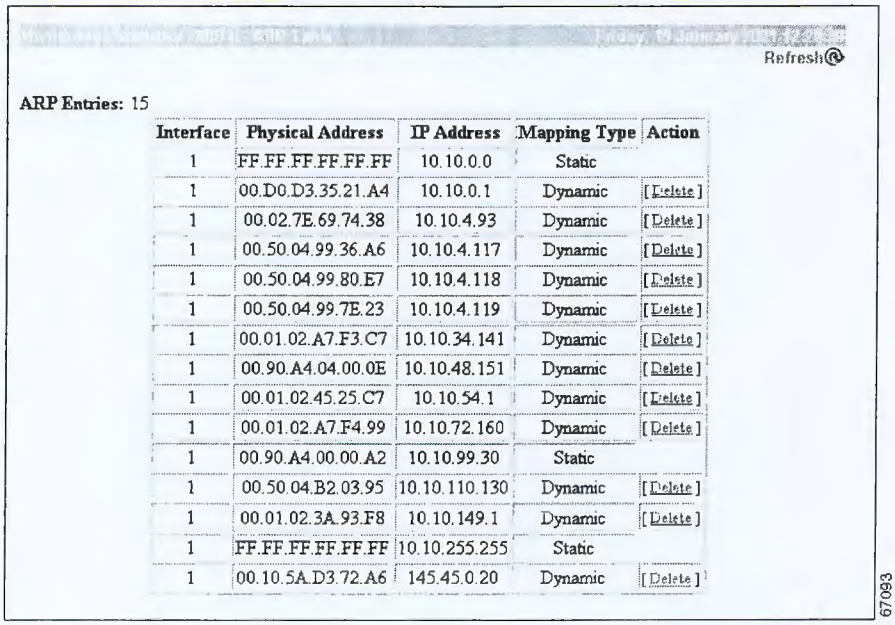
Monitoring | Statistics | MIB-II | ARP Table

This screen shows entries in the Address Resolution Protocol mapping table since the VPN Concentrator was last booted or reset. ARP matches IP addresses with physical MAC addresses, so the system can forward traffic to computers on its network. RFC 2011 defines MIB entries in the ARP table.

The entries are sorted first by Interface, then by IP Address. To speed display, the Manager might construct multiple 64-row tables. Use the scroll controls (if present) to view the entire series of tables.

You can also delete dynamic, or learned, entries in the mapping table.

Figure 17-32 Monitoring / Statistics / MIB-II / ARP Table Screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Arp Entries

The total number of entries in the ARP table.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0133
Doc 3690

14.662

Interface

The VPN Concentrator network interface on which this mapping applies:

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.
- 1000 and up = VPN tunnels, which are treated as logical interfaces.

Physical Address

The hardwired MAC (Medium Access Control) address of a physical network interface card, in 6-byte hexadecimal notation, that maps to the IP Address. Exceptions are:

- 00 = a virtual address for a tunnel.
- FF.FF.FF.FF.FF.FF = a network broadcast address.

IP Address

The IP address that maps to the physical address.

Mapping Type

The type of mapping:

- Other = none of the following.
- Invalid = an invalid mapping.
- Dynamic = a learned mapping.
- Static = a static mapping on the VPN Concentrator.

Action / Delete

To remove a dynamic, or learned, mapping from the table, click **Delete**. *There is no confirmation or undo.* The Manager deletes the entry and refreshes the screen.

To delete an entry, you must have the administrator privilege to Modify Config under General Access Rights. See Administration | Access Rights | Administrators.

You cannot delete static mappings.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0134
3690

Monitoring | Statistics | MIB-II | Ethernet

This screen shows statistics in MIB-II objects for Ethernet interface traffic on the VPN Concentrator since it was last booted or reset. IEEE standard 802.3 describes Ethernet networks, and RFC 1650 defines Ethernet interface MIB objects.

To configure Ethernet interfaces, see Configuration | Interfaces.

Figure 17-33 Monitoring / Statistics / MIB-II / Ethernet Screen

Refresh

	Errors						Collisions			MAC Errors				
Interface	Alignment	FCS	Carrier Sense	SQE Test	Frame Too Long	Deferred Transmits	Single	Multiple	Late	Excessive	Transmit	Receive	Speed (Mbps)	Duplex
Ethernet 1 (Private)	0	0	0	0	0	0	0	0	0	0	0	0	100	Half
Ethernet 2 (Public)	0	0	0	0	0	0	0	0	0	0	0	0	0	Half

67220

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The Ethernet interface to which the data in this row applies. Only configured interfaces are shown.

Alignment Errors

The number of frames received on this interface that are not an integral number of bytes long and do not pass the FCS (Frame Check Sequence; used for error detection) check.

FCS Errors

The number of frames received on this interface that are an integral number of bytes long but do not pass the FCS (Frame Check Sequence) check.

Carrier Sense Errors

The number of times that the carrier sense signal was lost or missing when trying to transmit a frame on this interface.

SQE Test Errors

The number of times that the SQE (Signal Quality Error) Test Error message was generated for this interface. The SQE message tests the collision circuits on an interface.

Frame Too Long Errors

The number of frames received on this interface that exceed the maximum permitted frame size.

Deferred Transmits

The number of frames for which the first transmission attempt on this interface is delayed because the medium is busy. This number does not include frames involved in collisions.

Single Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by exactly one collision. This number is not included in the Multiple Collisions number.

Multiple Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by more than one collision. This number does not include the Single Collisions number.

Late Collisions

The number of times that a collision is detected on this interface later than 512 bit-times into the transmission of a packet. 512 bit-times = 51.2 microseconds on a 10-Mbps system.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls
0136
3690
Doc

Excessive Collisions

The number of frames for which transmission on this interface failed due to excessive collisions.

MAC Errors: Transmit

The number of frames for which transmission on this interface failed due to an internal MAC sublayer transmit error. This number does not include Carrier Sense Errors, Late Collisions, or Excessive Collisions.

MAC Errors: Receive

The number of frames for which reception on this interface failed due to an internal MAC sublayer receive error. This number does not include Alignment Errors, FCS Errors, or Frame Too Long Errors.

Speed (Mbps)

This interface's nominal bandwidth in megabits per second.

Duplex

The current LAN duplex transmission mode for this interface:

- Full = Full-Duplex: transmission in both directions at the same time.
- Half = Half-Duplex: transmission in only one direction at a time.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0137
Doc 3690

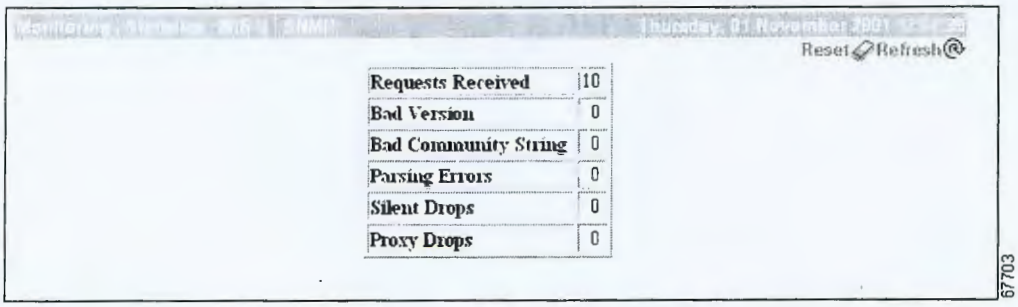
14,664

Monitoring | Statistics | MIB-II | SNMP

This screen shows statistics in MIB-II objects for SNMP traffic on the VPN Concentrator since it was last booted or reset. RFC 1907 defines SNMP version 2 MIB objects.

To configure the VPN Concentrator SNMP server, see Configuration | System | Management Protocols | SNMP.

Figure 17-34 Monitoring | Statistics | MIB-II | SNMP Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests Received

The total number of SNMP messages received by the VPN Concentrator.

Bad Version

The total number of SNMP messages received that were for an unsupported SNMP version. The VPN Concentrator supports SNMP version 2.

ROS Nº 03/2006 - CN
CPMI - CORREIOS
Fls. Nº 0138
Doc 3690

14.663

Bad Community String

The total number of SNMP messages received that used an SNMP community string the VPN Concentrator did not recognize. See Configuration | System | Management Protocols | SNMP Communities to configure permitted community strings. To protect security, the VPN Concentrator does not include the usual default public community string.

Parsing Errors

The total number of syntax or transmission errors encountered by the VPN Concentrator when decoding received SNMP messages.

Silent Drops

The total number of SNMP request messages that were silently dropped because the reply exceeded the maximum allowable message size.

Proxy Drops

The total number of SNMP request messages that were silently dropped because the transmission of the reply message to a proxy target failed for some reason (other than a timeout).

CORREIOS
Fls. Nº 0139
Doc 3690

14.662
J

Switch Tipo 5 doc 9

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0140
3690
Doc

34.697

White Paper

CiscoWorks **VPN/Security Management Solution** (VMS) 2.1 Deployment Guide

Introduction

The Challenge

One of the challenges of network management is the ability to have a solution that is flexible and can adapt to the changing needs of a network. While it makes sense to have applications that provide basic network management functionality regardless of function, the network environment must also be considered. In this case, it makes more sense to have a focused set of tools for management. For example, a tool that focuses on managing Quality of Service (QoS) levels is not necessarily (and most likely not) going to be very good at managing a server farm topology.

Growth and Enhancements in Network Security

If we look at the network as a strategic asset to the enterprise, network management clearly becomes an important factor in the success of the company. When we consider the evolution of business applications running across the traditional data network including e-commerce, business-to-business transactions, voice over IP (VoIP), the need to provide secure network connections grows. As a result, we have witnessed a proliferation in virtual private networks (VPNs) and an enhanced awareness of network security, setting the stage for reliable security management.

Paper Objective

The purpose of this paper is to provide guidance on how to effectively deploy CiscoWorks VPN/Security Management Solution (VMS). Covered topics include: server, installation, and operating system requirements; reference topology; metrics to monitor; and device configuration considerations. This is intended to supplement the CiscoWorks VMS Quick Start Guide and User Manual. We address such questions as: Which products are included and what are they used for? How many servers will be needed? What devices can be managed with this application? By answering these questions, we can provide some basic best practices for managing specific Cisco security technology.

What It Does Not Do

This paper does not replace User Guides (and other product documentation). It does not go into comprehensive detail about the various features or capabilities of the products.

Intended Audience

This paper is intended for audiences who are already familiar with network security, VPNs, firewalls, and intrusion detection. The audience should already have a basic understanding of these concepts and tools; our goal is to show how best to deploy CiscoWorks VMS in a production environment.

CPM
Dis N° 0141
Doc 5690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.660

High-level Overview of CiscoWorks VMS 2.1

What Does It Do?

The CiscoWorks VMS solution is a set of integrated tools that provide a comprehensive solution for VPN and security management. CiscoWorks VMS features are positioned for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based intrusion detection systems (IDS). VMS provides key features to assist customers in the deployment, monitoring, and management of their security-specific hardware. It also provides the operational management support, software distribution, configuration archive, change-audit, and syslog management for different elements of a Cisco security infrastructure. VMS provides a scalable solution that addresses the needs of small- and large-scale VPN and security deployments.

CiscoWorks VMS 2.1 Components

The CiscoWorks VPN/Security Management Solution (CiscoWorks VMS) consists of installable software components for flexible deployment options. Table 1 lists the different CiscoWorks VMS modules and their basic usages.

Table 1 CiscoWorks VMS 2.1 Modules

VMS Module	Usage
Auto Update Server	Permits configurations to be pulled from update server
CD-One/CiscoView	Provides graphical device management
Cisco IDS Host Sensor and Console	Configures host-based IDS to protect critical servers
Cisco Secure Policy Manager	Configures Cisco PIX Firewall, Cisco IOS Software firewall, and VPN
Common services	Provides a set of common software and services for the Management Centers
Management Center for IDS Sensor	Configures network-based IDS
Management Center for PIX Firewalls	Configures PIX Firewalls
Management Center for VPN routers	Configured VPN routers
Monitoring Center for Security	Monitors network and host-based IDS events, IOS and PIX syslog
Resource Manager essentials	Provides operational management, such as software distribution, change audit, syslog analysis
VPN Monitor	Monitors IPSec-based site-to-site and remote access VPN

These components can be classified into three distinct categories: Core asset management applications, monitoring applications, and security configuration applications. This section details some of the basic features associated with each product.

0142
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.659

Core Asset Management Applications

CD-One (CiscoView)

CD-One software provides the Common Management Foundation (CMF) for CiscoWorks. This includes basic components on the management server such as the web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed from CiscoWorks VMS since it is the prerequisite for other applications. In addition to the CMF, CD-One provides the web-based CiscoView application. CiscoView provides graphical browser-based access to real-time devices status and simple network management protocol (SNMP) configuration capabilities.

CiscoWorks Resource Manager Essentials

CiscoWorks Resource Manager Essentials (RME) provides the basic network management tools for day-to-day network management, including inventory, configuration, change audit, and syslog. RME also provides additional VPN management capabilities. Network administrators can now produce device configuration, software image, and syslog reports specific for VPN environments.

Security Monitoring Applications

CiscoWorks VPN Monitor

CiscoWorks VPN Monitor allows users to monitor the status of their VPN devices and tunnels. This application collects, stores, and reports statistics for VPN-capable devices, including Cisco VPN routers, and the Cisco VPN 3000 Series Concentrator. The VPN Monitor supports the two major classes of VPNs (site-to-site and remote access) as well as multiple tunneling protocols, including Layer 2 Tunneling Protocol, Point-to-Point Tunneling Protocol (PPTP), and IP security (IPsec).

CiscoWorks Monitoring Center for Security

The CiscoWorks Monitoring Center for Security, or Security Monitor, monitors IDS events from various Cisco devices. These include network IDS sensor appliances, Cisco Catalyst® 6000 IDS modules, Cisco IOS® Software IDS syslog messages, Cisco PIX® Firewall syslog messages, and Cisco host IDS events.

Security Configuration Applications

CiscoWorks Common Services Software

CiscoWorks Common Services Software includes basic components of the management server such as the Web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed because it is the prerequisite for the Management Center tools in the CiscoWorks VMS bundle.

CiscoWorks Management Center for VPN Routers

CiscoWorks Management Center for VPN Routers (Router MC) is a VPN configuration and deployment tool for Cisco VPN routers with Cisco IOS Software. Router MC is a Web-based application installed on top of Common Services.

FOLIO
0143
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

JU.658

CiscoWorks Management Center for PIX Firewalls

Management Center for PIX Firewalls (PIX MC) is a complete firewall and access rule policy configuration tool for Cisco PIX Firewalls. You can configure new Firewalls and import configurations from existing firewalls. PIX MC also provides a powerful tool for controlling changes made to your network, showing configuration and status changes. PIX MC is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Auto Update Server

The CiscoWorks Auto Update Server (AUS) is used to store and upgrade device configuration files and software images. Cisco PIX Firewall devices periodically contact the AUS to request configuration and software updates. In this way, PIX Firewall devices are actively kept up to date. AUS is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Management Center for IDS Sensors

CiscoWorks Management Center for IDS sensors (IDS MC) is an IDS configuration and deployment tool for Cisco IDS sensor appliances and Cisco IDS Modules. IDS MC is a web-based application installed on top of Common Services.

Cisco IDS Host Sensor

Working as a complementary technology to IDS MC and Security Monitor, the Cisco Host Intrusion Detection System (HIDS) application protects critical servers and hosts by integrating with the operating system. By intercepting system calls to the kernel, Cisco HIDS software can protect the users' hosts by identifying attacks and preventing access to resources and unauthorized transactions.

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) is a policy-based application that allows network and security administrators to define and deploy perimeter security policies on mixed Cisco PIX Firewalls and Cisco IOS routers with the firewall feature set. CSPM also facilitates the deployment of site-to-site, mixed-environment VPN topologies.

Reference Topology

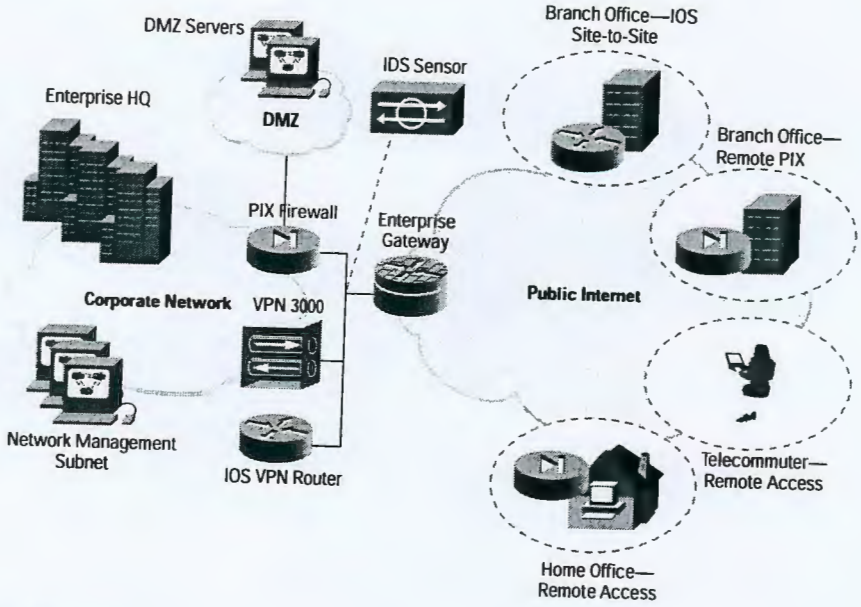
In order to describe how best to deploy the CiscoWorks VMS, we will use a reference network topology that shows the different aspects of VPN and network security (Figure 1). While obviously not identical to most customer environments, it does serve to provide a holistic view of a secure network. The intent is that by providing this reference, readers will be able to select the different components that best represent their topology and hence, understand how best to deploy CiscoWorks VMS in their environment.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0144
Doc. 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.657

Figure 1
Reference Security Topology



The infrastructure involved:

a. Enterprise Gateway: This is a Cisco IOS router with the firewall feature set. The main purpose of this device is to perform the gateway routing and the basic frontline firewall functionality.

b. Cisco PIX Firewall: The Cisco PIX Firewall provides the comprehensive firewall functionality for this enterprise network. By strategically placing these devices at network access points, the corporate network resources are protected as a result of this firewall.

c. Cisco 800, 1700, 2600, 3600, 7100 or 7200 Series routers: Cisco routers act as site-to-site VPN termination points. In a hub-and-spoke VPN topology, the high-end VPN routers act as hubs, and the small- to medium-sized routers act as spokes.

d. Cisco VPN 3000 Series Concentrator: The VPN 3000 Series Concentrator is designed to provide scalable remote access VPN termination. In this topology the concentrator terminates VPN connections with a variety of remote access environments, VPN client software, and tunneling protocols (IPSec, L2TP, PPTP).

e. Cisco VPN remote-access client software: This software allows remote access users to connect to the corporate network via VPNs.

f. Cisco IDS Network Sensor: This device sits on a network segment and passively "listens" to the traffic, inspecting it against a database of common attack signatures. It forwards IDS event information to the monitoring station.

g. Cisco host-based IDS agents: Software that sits on critical network servers that protect individual hosts from intrusion and attacks. Events are forwarded to a central monitoring console.

h. Network Management Subnet: This subnet represents a dedicated network segment for the network management servers. The components of CiscoWorks VMS will reside in this subnet to manage the different pieces of the infrastructure.

0145
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.656

i. Demilitarized zone (DMZ) Servers: This subnet represents a dedicated network segment for publicly accessible network servers. Generally, this includes e-mail, Web, File Transfer Protocol (FTP) servers, and in our case will include the Auto Update Server.

Within our reference topologies, we will be focusing on several pieces of the infrastructure that CiscoWorks VMS manages. That is not to say that the network management applications within VMS cannot manage other pieces (such as Cisco Catalyst switches), but these are the components that should be the focal point of VMS. These components include:

Enterprise HQ

This includes the network management servers, internal firewalls, VPN termination points (both hub routers and VPN concentrators), and IDS sensors. Access to the DMZ portion of the network will be controlled by internal firewalls and also have publicly accessible servers.

Remote Access Sites

The remote access sites in our topology contain the remote Cisco PIX Firewalls, remote IOS VPN routers, and remote VPN clients. These pieces of the infrastructure are responsible for VPN termination and firewall access policy at the remote site.

Software Requirements for CiscoWorks VMS

CiscoWorks VMS is composed of a series of tools that reside on a network management server (or servers). This section covers the prerequisite software needed in order to install and run the components within VMS. Primarily, this refers to operating system (OS) support. For almost every application in the VMS bundle, the supported OS is Windows 2000 Professional or Server. This is summarized in Table 2.

Table 2 Supported OS for CiscoWorks VMS Modules

CiscoWorks VMS Module	Windows Support	Solaris Support
CD-One	X	X
Resource Manager Essentials	X	X
VPN Monitor	X	X
Common Services	X	
Management Center for PIX Firewalls	X	
Auto Update Server	X	
Management Center for VPN routers	X	
Management Center for IDS Sensor	X	
Monitoring Center for Security	X	
Cisco IDS Host Sensor and Console	X[1]	
Cisco Secure Policy Manager	X	

1. Windows NT 4.0 Server, Enterprise Server (SP4 or later), Windows 2000 Advanced Server

0146
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.655

To run the CiscoWorks VMS components on a Windows 2000 system, the following requirements must be considered:

- Windows 2000 (Service Pack 2 or later)
- IE 5.5 SP2 or later
- ODBC Driver Manager 3.510 or later
- NTFS File System
- Do not install VMS on a server that is a:
  - Primary domain controller
  - Backup domain controller
  - Terminal server

Mitigating Threats

Now that we have the basic hardware and software requirements, we must consider how to configure the servers themselves to be ready for management. As a general security axiom, to secure hosts, pay careful attention to each of the components within the systems. Keep all systems up to date with the latest patches, fixes, and so forth. In the particular case of VMS, it is important to have the latest Windows 2000 patches and hot-fixes for security. Following is a detailed checklist of items to make sure the Windows 2000 server is ready to be used as a management server:

- Install the operating system on its own partition
- Use strong passwords
- Avoid creating network shares
- Disable unnecessary accounts
- Secure the Registry
- Apply all hot-fixes and security patches
- Disable unused and unneeded services (at a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug & Play, Protected Storage, and Security Accounts Manager. Do not install IIS.)
- Disable all network protocols except Internet Protocol (TCP/IP)
- Monitor the security of your system regularly
- Limit physical access to your server
- Do not install remote access or administration tools on the server
- Periodically run a virus scanning application on the server

Hardware Considerations for CiscoWorks VMS

Along with the software requirements, be aware of the hardware requirements for the CiscoWorks VMS bundle. Then the inherent challenge is deciding how best to deploy the different applications in the solution. Since there are eleven installable software applications, there are numerous combinations in which to deploy them.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0147
Fls. Nº
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14,654

Platform and Specs

The following server system requirements are specified in the VMS bundle documentation:

- Pentium III 1GHz CPU
- 1 GB RAM
- 2 GB virtual memory
- 9 GB free hard disk space

These are minimum requirements, and consideration should be given to the difference in recommended system specifications based upon different sized networks and configurations. For example, consider three different sized configurations: small, medium, and large. The first thing to think about is scalability. In other words, how many devices equate to a small, medium, and large configuration?

Scaling

Each application within CiscoWorks VMS has a different scalability metric. Table 3 provides the theoretical maximum for each of the applications.

Table 3 Theoretical Scale Limits for CiscoWorks VMS Applications

CiscoWorks VMS Module	Scalability Metric (tested up to[1])
IDS MC	300 IDS sensors
Security Monitor	500 events/sec[2]
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices
RME	5000 devices inventory, 1000 devices availability
VPN Monitor	30 devices on dashboard (hard limit)
Cisco IDS Host Console	300 host agents

1. The theoretical scale limits define what the tools have been tested up to. The numbers are stated as a guideline to guarantee reasonable performance and user experience. Although possible, it is not recommended to exceed these metrics.
2. If the volume of security events exceeds 500/second for extended periods of time, it is recommended that users consider a monitoring product from a partner-vendor that can handle higher event volumes.

These are not software-imposed limits, but rather the scale limitations based on testing maximums. For example, if a user wants to add device number 1001 to Router MC, the software will allow it. However, from a support standpoint, we do not recommend doing this.

Also note that the specifications for the minimum recommended hardware system for CiscoWorks VMS are based on testing and performance statistics for ONE (not all) of the applications in the bundle. For example, if you are using IDS MC to manage 300 sensors (the theoretical maximum), we do NOT recommend using any other applications on that server. If you plan to heavily use more than one application within VMS, it is highly recommended to put them on separate servers.

0148
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14,653

The following tables list some of the more resource-intensive applications within the bundle, and configuration is broken down into small, medium, and large configuration metrics in Tables 4-6, respectively.

Table 4 Small Configuration Metrics (reflects restricted CiscoWorks VMS license model)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	20 IDS sensors
Security Monitor	200 events/sec
PIX MC	20 PIX Firewalls
AUS	20 PIX Firewalls
Router MC	20 VPN routers
CSPM	20 devices

Table 5 Medium Configuration Metrics (This configuration represents the majority of the CiscoWorks VMS customer base):

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	100 IDS sensors
Security Monitor	300 events/sec
PIX MC	100 PIX Firewalls
AUS	100 PIX Firewalls
Router MC	100 VPN routers
CSPM	50 devices

Table 6 Large Configuration (Reflects the theoretical maximum scalability metrics.)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	300 IDS sensors
Security Monitor	500 events/sec
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices

0149

Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.652
1

Server Sizing

Based on these factors, a closer examination of the recommended server sizing for each configuration is now possible. It is important to note that these specifications are minimum requirements for individual applications and are frequently exceeded in many deployments. The general rule of thumb here is, if it is necessary to choose one metric that will have the greatest affect on performance, then increase the amount of RAM. It is also important to pay attention to the scale limits of each application. If you are approaching some of those theoretical limits, it might be a good idea to increase the horsepower of your VMS server(s). For example, it is not out of the question to see a P4 2.2GHz CPU with 4 GB of RAM running VMS applications. For a general guideline, please see Table 7.

Table 7 Server Recommendations for CiscoWorks VMS Configurations

Configuration	Small	Medium	Large
CPU	PIII 1GHz	PIII 1.4GHz	P4 2.0GHz
RAM	1 GB	1.5 GB	2 GB
Virtual memory	2 GB	3 GB	4 GB
Hard disk space	9 GB	20 GB	40 GB

Server Deployment Rules of Thumb

In terms of application compatibility, there are several rules to follow:

- CD-One, RME, and VPN Monitor MUST reside on the same server.
- Router MC, IDS MC, Security Monitor, PIX MC, and AUS must be installed on top of Common Services. However, since more than one instance of Common Services can be installed, these can still be deployed across different servers.
- CD-One MUST be installed before Common Services.

Given these conditions, CiscoWorks VMS can have extremely flexible deployments. All of the components can be installed and run on a single server. On the other side of the spectrum, each of these components can be installed on its own individual server. This extreme is not practical and deployment will generally depend on a number of factors, including the following four:

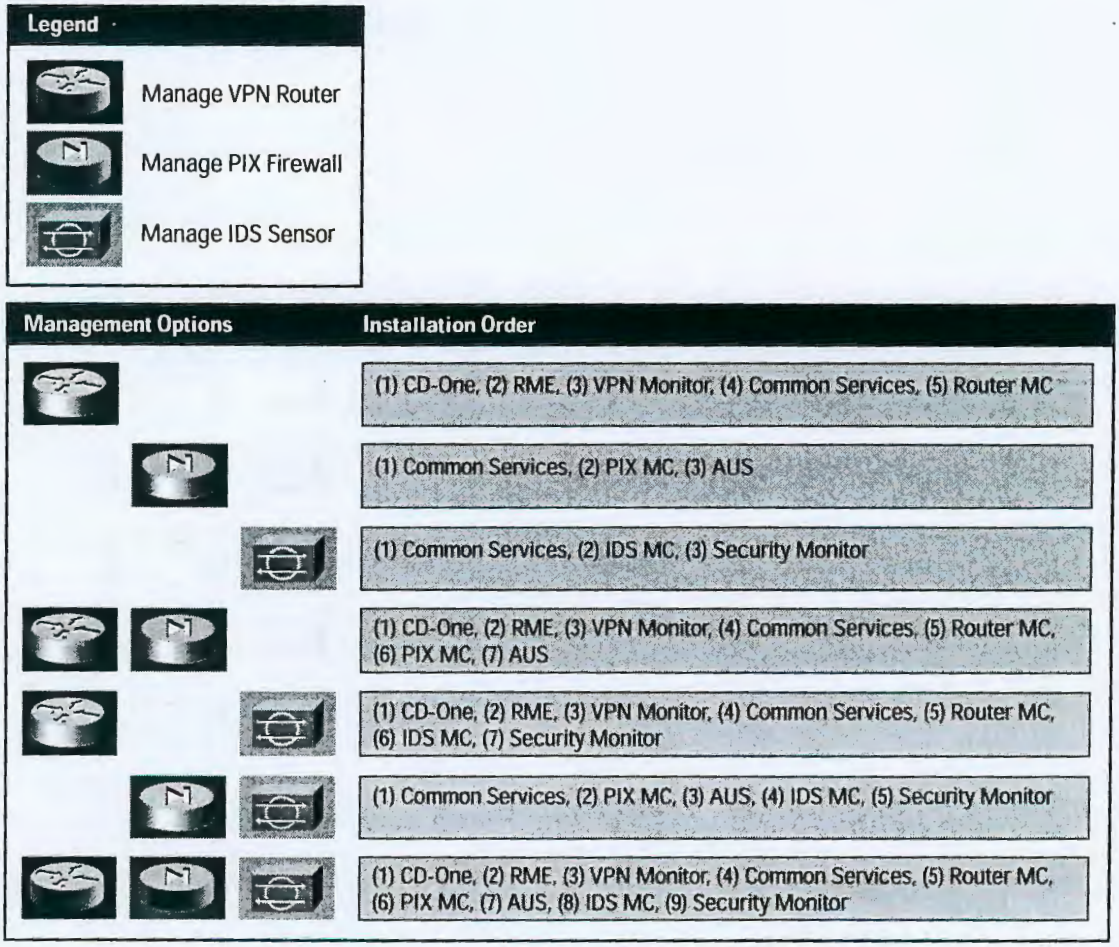
1. Which applications do you actually need?

Although VMS provides a rich, comprehensive management solution, it is possible (and perhaps even probable) that users will not need every single tool. The first question that should be asked is: Which applications do I actually need? Once this has been determined, users can choose to install only the modules that are needed. Figure 2 shows a table that provides the installation order based upon the different management options provided they are installed on a single server.

0150
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 2
CiscoWorks VMS Module Installation Matrix



Note: This table provides basic guidelines. Obviously, not all the combinations and tools within VMS are covered—just those with installation order dependencies.

- Installation Option 1: For VPN management, it is the monitoring component that is covered by CD-One, RME, and VPN Monitor. If monitoring is not necessary, these modules do not need to be installed.
- Installation Option 2: For PIX management, AUS is only necessary in order to take advantage of the auto-update feature for PIX configuration and software deployment.

0151
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.650

2. How many devices will each application manage?

If one of the applications being used is approaching its theoretical scale limits, it is a good idea to dedicate a server to that application. For obvious reasons of resource allocation and task distribution, it is best not to have other applications using valuable CPU resources when trying to manage a large number of devices.

For example, if an instance of PIX MC is installed that is managing 800 PIX Firewalls, and the user is also trying to roll out a hub and spoke VPN deployment across 600 router spokes, it is probably a good idea to break these applications apart onto dedicated servers.

3. How many administrators will me using these applications?

In some multi-administrator environments, it makes sense to explore different deployment options for VMS. Because there are so many applications involved, and they each have a very distinct purpose, it is possible that there will be different security administrators using different applications. In this case, it is probably better to split these applications onto dedicated servers. This way, if one application is busy with a resource-intensive task such as generating configuration files, the second application will not suffer any degradation in performance.

4. What types of cost restrictions exist in terms of server procurement?

Does the organization using CiscoWorks VMS have (or have the ability to get) multiple servers? In some cases, there may only be enough budget to allocate to one server. If this is the case, then it is always better to shoot for a high-end server that exceeds the minimum system requirements. This allows room for growth, as well as improved performance.

More is Better

The bottom line is, if at all possible, use multiple servers and split the applications across them as they make sense. Generally, for better scalability, resource allocation, task distribution, and room for growth, more is better as long as it doesn't become cumbersome and unmanageable. Also keep in mind that if you decide to combine multiple applications onto a single server, you will need to pay special attention to the hardware requirements of each application and adjust accordingly.

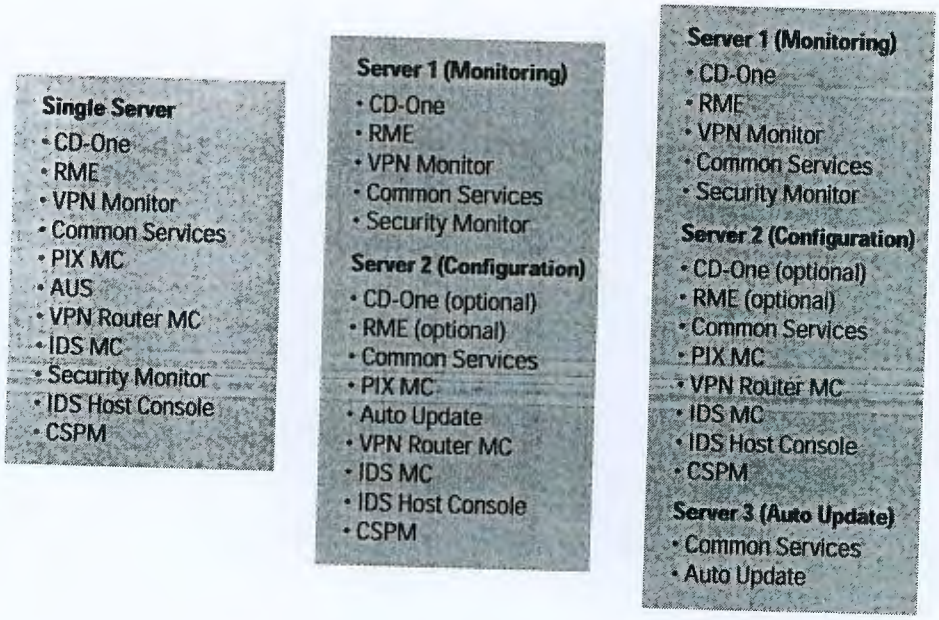
The following figure and section breaks down some basic deployment options and provides some general guidelines covering most customer scenarios (Figure 3). Note that these are simply recommendations, and do not necessarily indicate that CiscoWorks VMS must be deployed in this manner.

RQS nº 03/2005 - CN
CPMI - 0152
Fls. Nº
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.649

Figure 3
Server Deployment Options



Option 1: Single Server Deployment

For small-scale security environments with a single network security administrator, a single server deployment is recommended. This has the benefit of being low cost to the organization and guarantees ease of administration.

Option 2: 2 Servers: Configuration and Monitoring

This deployment option breaks down the VMS applications across function. One server is dedicated for monitoring and the second server is dedicated for configuration.

Server 1: Configuration

This security management server is designed to combine all of the CiscoWorks VMS applications that assist in configuration. Whether the infrastructure is VPN Router, PIX Firewall, IDS Sensor, or Host IDS Agent, this server's primary function will be configuration. The relevant applications are:

- Common Services
- PIX MC
- AUS[1]
- VPN Router MC
- IDS MC
- Cisco Host IDS Console
- Cisco Secure Policy Manager (CSPM)

ROS nº 03/2005 - CPMI - CORREIOS
Fls 0153
Doc 3690

1. AUS primarily provides configuration and software updates to remote PIX Firewalls. For this reason, it is frequently recommended to place the AUS within the organization's DMZ. If this is the case, we recommend using a dedicated server for AUS.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.648

Server 2: Monitoring

The second server in this deployment option is dedicated for monitoring. VPN Monitor is used for IPsec MIB monitoring and Security Monitor is used for consolidated event viewing of Post Office IDS, Host IDS, PIX, and IOS Syslog messages. The applications for this server are:

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Option 3: 3 Servers: Security Application Function

The third deployment option centers around splitting up the CiscoWorks VMS application according to security technology (or infrastructure) managed. The first server deals with VPNs, and generally this covers IOS-based VPN routers. The second server contains the applications used to manage the PIX Firewall. Finally, the third server is dedicated to the management and monitoring of IDS—both network-based and host-based IDS.

Server 1: VPN

- CD-One
- RME
- VPN Monitor
- Common Services
- VPN Router MC

Server 2: Firewall

- Common Services
- PIX MC
- AUS
- CSPM

Server 3: IDS

- Common Services
- IDS MC
- Security Monitor
- Cisco Host IDS Console

0154
Fls. Nº
3600

Option 4: 4 Servers: Granular Management Control

For greater granularity and scalability benefits, further divide the deployment. The main difference with this option is the use of a dedicated server for AUS, since it is placed within a different subnet of the network. The other difference is the use of a dedicated server for the policy management tool CSPM. This makes sense because CSPM does not have any natural integration with the other products in the bundle and it is also resource intensive. As such, it is recommended to split it up and have a dedicated system for policy management across mixed environments.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Server 1: Configuration

- Common Services
- PIX MC
- VPN Router MC
- IDS MC
- Cisco Host IDS Console

Server 2: Monitoring

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Server 3: Remote Management (placed in DMZ)

- Common Services
- AUS

Server 4: Policy

- CSPM

Again, keep in mind that these are only recommendations. There are numerous combinations and deployment options available and each case should be considered on an individual basis. There will likely be many cases where customers don't even want to use all of the possible applications within VMS.

CiscoWorks VMS Applied

Now that we have determined how to deploy the components of CiscoWorks VMS from an installation perspective, we need to take a look at how these applications should be deployed from a functional standpoint. Three basic questions will be addressed in this section:

1. What is the management function of each application?
2. What devices can I manage?
3. What types of services do I need to enable?

The first question requires a detailed look into the capabilities of each product. This information is used to figure out what aspects of security management can and should be managed by each of the components within VMS. Answering the second question will clarify confusion surrounding the variances in device support by the component applications. Finally, the last question looks at how each application touches the device(s) that it manages. By examining the communication protocols being used, we can compile a list of requirements that ensures a successful deployment of VMS. For the sake of clarity, we will examine each of the questions on a product/server basis.

Note: The components of a Cisco network infrastructure are diverse and varied; however, for this discussion surrounding security, we will focus on five classes of objects: IOS routers, PIX Firewalls, VPN concentrators, IDS sensors, and IDS host agents. This does not imply that VMS is not able to manage other elements, simply that these are the pieces we must pay special attention to for security issues.

CPMI 0155
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.646

A Word About Management Subnets (Out-of-Band Management)

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices that it is trying to manage. So when making this decision, consider that, while it might be desirable to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

CD-One (CiscoView)

What is the management function?

CiscoView provides graphical Web-based device management. Users of CiscoView see a graphical representation on their computer screen and are able to monitor real-time device status, and in certain cases make configuration changes to those devices. From a CiscoWorks VMS perspective, CiscoView is positioned as a troubleshooting tool. If there is a problem within the network, and that problem has been isolated to a single device or interface, then CiscoView can be used to take a look at the statistics associated with that device and potential configure variable(s) to solve the problem.

What devices does it manage?

CiscoView provides support for the majority of the Cisco IOS routers, Cisco VPN 3000 Series Concentrators, and the Cisco PIX Firewall 501 and 506 Series.

Which services do I need to enable? (Application protocol requirements)

CiscoView relies entirely on SNMP get/set operations (UDP port 161) for its functionality. From the CiscoView server to the device, you need to enable SNMP traffic. Furthermore, the devices that you are managing must be configured to support SNMP. The Cisco IOS Software devices can support both get and set operations (for both monitoring and configuration), so both read and write community strings are configured separately to provide this level of granularity. For the VPN 3000 Concentrators and the PIX Firewalls, only SNMP read operations are supported—so while you can monitor these devices, configuration using CiscoView is not possible.

Resource Manager Essentials

What is the management function?

Describing the functions of Resource Manager Essentials (RME) would take an entire paper by itself. In general (and from a security perspective), this application provides basic network management operations and administration. Basically, this tool provides:

- Inventory management to keep track of the devices within the infrastructure
- Configuration management to manage configuration of the network devices
- Change audit control to keep track of any changes (configuration or otherwise) occurring in the network
- Software image management to facilitate the maintenance of software versions
- Syslog management to receive and analyze syslog messages sourced from the network devices

Fls. Nº 0156
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14,645

This list confirms that RME functionality provides benefits beyond the scope of security infrastructure management. For the purposes of this discussion, focus is on the benefits it provides to our reference environment. Of special interest is the fact that RME can generate configuration reports, software image upgrade analysis, and syslog reports specific to VPN-related infrastructure and environments.

What devices does it manage?

RME provides support for Cisco IOS routers, VPN 3000 Concentrators, and PIX Firewalls (506, 515, 520, and 525 Series). For the concentrators, RME does NOT support configuration management and only provides limited support for software image management. For the PIX Firewalls, RME provides limited support for syslog management. Refer to the diagram of our reference topology and notice this covers all aspects of our network with the exception of the IDS sensor. For this reason, RME is frequently referred to as our "core" management application.

Which services do I need to enable? (Application protocol requirements)

RME depends on several protocols to manage its devices. These include SNMP, Telnet, TFTP, and Syslog, among others. Because the subcomponents of RME are so varied, along with the different devices, we've summarized the application protocol requirements for this tool in Table 8.

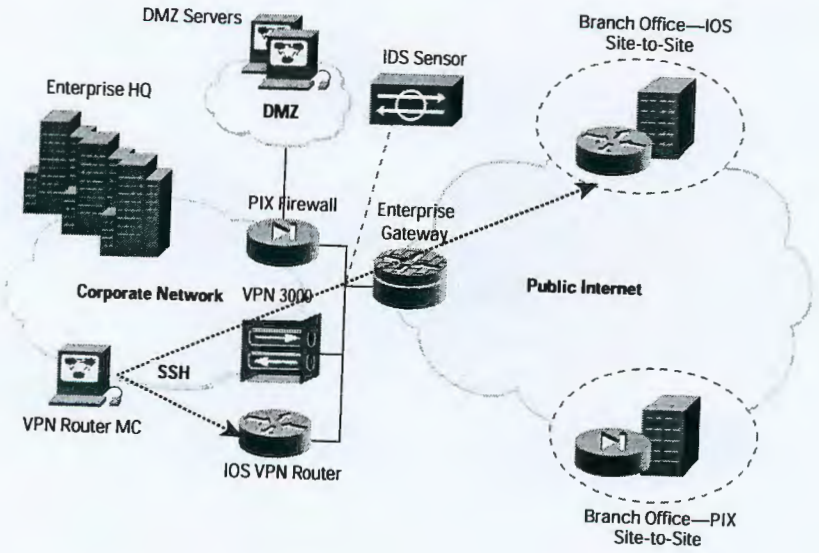
Table 8 CiscoView and RME Protocol Requirements

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

Fls. Nº 0157
Doc 3690

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 5
PIX MC Applied



Auto Update Server

What is the management function?

AUS is responsible for storing configurations and software images for PIX Firewalls. Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS. Using AUS also facilitates managing devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP) or that sit behind Network Address Translation (NAT) boundaries. Typically, because of this management function, the AUS is deployed in a publicly accessible DMZ which the remote side PIX Firewalls can contact directly.

What devices does it manage?

PIX MC is used to manage the PIX Firewalls deployed throughout your network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. AUS requires that PIX Firewalls run OS version 6.2 since it requires the Auto Update feature.

Which services need to be enabled? (Application protocol requirements)

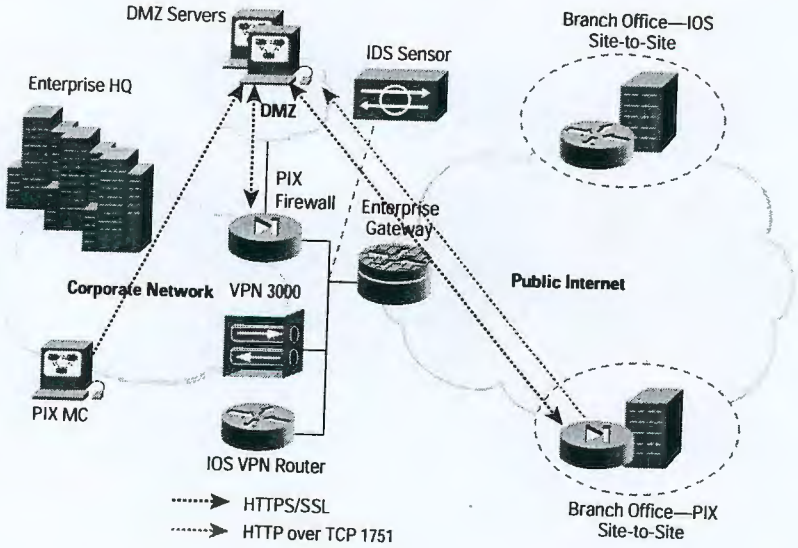
AUS talks to two different pieces in our topology diagram. The first piece it talks to is the PIX MC server. If these two applications are installed on the same system, no changes are necessary to the communication architecture. However, if they are installed on different servers, the PIX MC server will push configuration files to AUS using SSL, making it necessary to open up TCP 443 to the AUS system.

0158
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The second piece is the actual communication between the AUS and the PIX Firewall itself. In this scenario, there is two-way communication and both occur via SSL. Therefore, it is not only necessary to open up TCP 443 to the AUS from the PIX, but also vice versa. For transfer of binary images (PIX and PDM software), this will be transferred via standard HTTP over TCP 1751 (this can optionally be changed to SSL). Figure 6 illustrates how AUS is applied to our reference topology.

Figure 6
AUS Applied



Management Center for IDS

What is the management function?

Management Center for IDS (IDS MC) manages configurations for Cisco Intrusion Detection System Sensors. All aspects of sensor configuration can be managed through a series of Web-based screens, including individual sensors or a group of sensors having a common configuration. The sensor configuration data resides in a database. IDS MC can also perform signature updates by downloading the update archives from the Cisco web location and then distributing these signature updates to the appropriate sensor groups.

A separate but closely related product, Monitoring Center for Security (Security Monitor), provides event collection, viewing, and reporting capability for network devices. This is covered in the next section.

0159
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.639

What devices does it manage?

IDS MC manages the Cisco IDS appliance sensors as well as the Cisco IDS Module for the Catalyst 6500. The IDS software required for the application depends on the platform (See Table 10).

Table 10 Required IDS Sensor Software for IDS MC

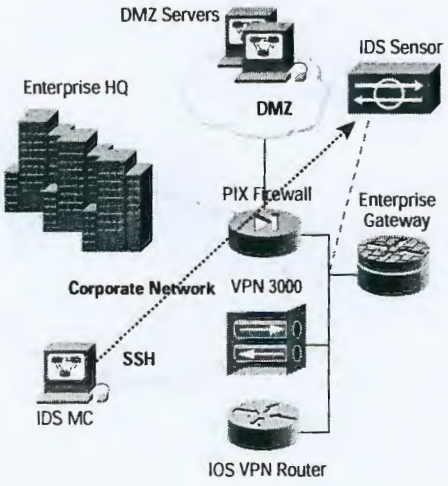
IDS Sensor Platform	Minimum Required Software
Cisco IDS Appliance Sensor	3.0.1[1]
Catalyst 6000 IDS Module	3.0.5[1]

1. IDS 4.0 software will be supported in a future release of IDS MC and Security Monitor.

Which services need to be enabled? (Application protocol requirements)

IDS MC uses two protocols to manage the IDS sensors: First, it uses Secure Shell (SSH) to secure remote login to the sensors. Second, it uses SCP to secure the transfer of the actual sensor configuration files. Session-Control Protocol (SCP) uses SSH for data transfer, so TCP 22 needs to be allowed to the sensors. Figure 7 illustrates how IDS MC is applied to our reference topology.

Figure 7
IDS MC Applied



Security Monitor

What is the management function?

Monitoring Center for Security (Security Monitor) provides a Web-based interface for event collection, viewing, and monitoring for the following devices:

- Cisco Intrusion Detection System Sensor running Post Office software
- Cisco IOS router running IDS software
- Host IDS Sensor via the Console
- PIX Firewall

0160
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Security Monitor displays events on a customizable event viewer, and allows the user to write some basic event correlation rules to consolidate events. These rules can also be set up to kick off real time notifications.

What devices does it manage?

Security Monitor can receive security events from five sources with the following software requirements:

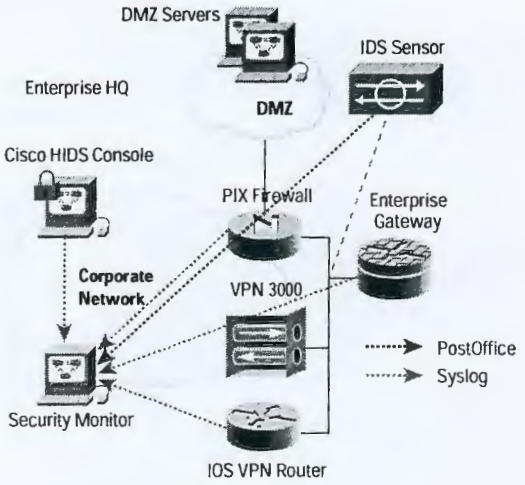
Table 11 Required Software for Security Monitor Devices

Security Event Source	Minimum Software Required
Cisco IDS Appliance Sensor	3.0.1
Catalyst 6000 IDS Module	3.0.5
IOS router	IOS with IDS features set
PIX Firewall	Any version that supports syslog
Host IDS Console	2.5 or later with integrator software

Which services do I need to enable? (Application protocol requirements)

Because of the number of data inputs, consider each of these individually in terms of application protocol requirements. For the Post Office devices (sensor appliance and IDS module), Security Monitor uses Post Office protocol to forward events. For the other data sources (Cisco IOS Software, PIX and Host IDS), the events are sent to Security Monitor via syslog. So make sure to allow Post Office (UDP 45000) and syslog (UDP 514) to the Security Monitor server. Figure 8 illustrates how Security Monitor is applied to our reference topology.

Figure 8
Security Monitor Applied



0161
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

JM. 637

VPN Monitor

What is the management function?

VPN Monitor provides monitoring statistics for the enterprise head-end VPN devices—this means the "hubs" of a hub-and-spoke VPN topology. In our reference topology, this refers to both the Cisco 7X00 Series Router and the VPN 3000 Concentrator, so proper connectivity from the VPN Monitor server to those devices is necessary. This application provides statistical VPN information in both graphical and tabular format. It can also be used as a graphical notification tool when certain VPN-related thresholds (that are user configurable) are violated. With VPN Monitor, network administrators can get an overall view of how their VPNs are doing by looking at metrics that include encrypted traffic statistics, secure handshake negotiations, packet replays, and so on.

What devices does it manage?

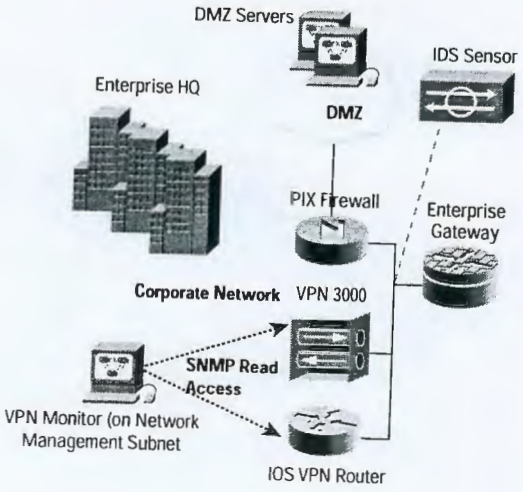
VPN Monitor supports Cisco IOS VPN routers with the necessary IPSec MIB support as well as VPN 3000 Concentrators. Currently, the application supports the Cisco1700, 2600, 3600, 7100, and 7200 Series routers. The software image version requirements are:

- 1700, 2600, or 3600 IOS Router—12.2(4)T or later
- 7100 or 7200 IOS Router—12.1(5a)E or later
- VPN Concentrator 3000 Series—2.5.2f or later

Which services do I need to enable? (Application protocol requirements)

Much like CiscoView, VPN Monitor requires SNMP (UDP port 161) to function. The VPN Monitor server periodically polls the devices to retrieve the IPSec MIB information. Since this is purely a monitoring tool, it is only necessary to consider SNMP get operations on these two classes of devices. This corresponds to configuring the SNMP read community string on the network devices that need to be managed with VPN Monitor. Figure 9 illustrates how VPN Monitor is applied to our reference topology.

Figure 9
VPN Monitor Applied



Fls. Nº 0162
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

$4636

Note: Given these requirements, it IS possible to use VPN Monitor on a remote VPN device. However, this is not entirely practical for two reasons: First, this type of monitoring does not scale as well. Second, in most cases it is sufficient to view the VPN metrics from one end of the tunnel (and not both).

Cisco IDS Host Sensor

What is the management function?

The Cisco IDS Host Sensor (Cisco HIDS) application is a product that complements the network-based IDS management provided in IDS MC and Security Monitor, and gives CiscoWorks VMS a truly comprehensive solution to manage intrusion detection. The basic premise of Cisco HIDS is to protect individual host systems from intrusion detection. The software (agent) sits on the host itself and examines system calls to the OS kernel, comparing these to a database of well-known signatures. Events are reported back to a central Cisco HIDS Console system, which consolidates the information from the agents it is managing. If a signature match is found, Cisco HIDS will prevent the operation and shoot off a real-time notification.

This protection model is proven to mitigate well-known threats such as the NIMDA and Code-Red worms without any user configuration. This means the Cisco HIDS agent software is especially important to use on important network hosts, at the user's discretion. In our reference topology, the Cisco HIDS agent code is installed on all the network management servers that comprise the VMS solution, thus protecting the important network management systems. These servers report IDS events back to the HIDS Console system, which are then forwarded to Security Monitor, provided the integrator software is installed on the HIDS Console. Users are asked to provide the IP address and syslog listening port of Security Monitor during the installation of the integrator.

What devices does it manage?

The Cisco HIDS application does not directly interact with Cisco network devices. It interacts with network hosts with the Cisco HIDS Agent code installed. At present, the following server OS versions are protected:

- Windows NT 4.x Server
- Windows NT Enterprise Server (SP 3 or later)
- Windows 2000 Server
- Windows 2000 Advanced Server
- Solaris 2.6, 2.7, and 2.8

The following Web servers are protected:

- Windows IIS Web Server
- Solaris Apache
- Solaris Netscape Enterprise
- Solaris iPlanet

Consult product documentation to verify the current available option of the Cisco HIDS Agent software.

CORREOS - C.I
CHILE - CORREOS
Fs. Nº 0163
Doc 3690

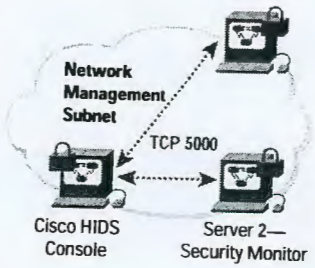
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.635

Which services do I need to enable? (Application protocol requirements)

For Cisco HIDS to work properly, the agents must be able to communicate with the console. This is necessary so that the agents can report IDS events to the console, and just as importantly, the console can push configuration changes out to the agents. This communication is accomplished through a proprietary protocol that travels on TCP port 5000. This port number is actually a configurable option upon install, but TCP port is the default value. Figure 10 illustrates how the Cisco HIDS application is applied to our reference topology.

Figure 10
Cisco HIDS Console and Agents Applied



Cisco Secure Policy Manager

What is the management function?

Cisco Secure Policy Manager (CSPM) is an end-to-end security policy tool. Network administrators use CSPM to define and deploy security policies for their networks. This can be something as simple as what hosts or networks are allowed to access their network, or it can be something much more complex involving encryption, access methods, and other variables. The point is that, using CSPM, network administrators can implement policy management across their mixed network infrastructures.

From the perspective of our reference topology, the role of CSPM is twofold: 1. It manages traffic encryption policy by handling the VPN configuration that allows the user to configure the hub and spoke VPN tunnels between the 7X00 Series Router on the corporate network to the endpoints on the branch sites (both IOS and PIX devices). 2. It allows the user to configure security policies on the PIX Firewall(s) and also the firewall feature set on the IOS enterprise gateway, defining basic firewall policy distribution.

What devices does it manage?

As can be inferred from the previous paragraph, CSPM is able to manage the Cisco IOS routers and PIX Firewalls. The software image version requirements are:

- Cisco IOS Router—12.0(5) or later with the FW-DES feature set
- PIX Firewall—4.2.4 or later with the Data Encryption Standard (DES) feature set

Other versions can be added and managed as well, using the version management utility in CSPM.

CORREIOS
Fls. Nº 0164
Doc 3690

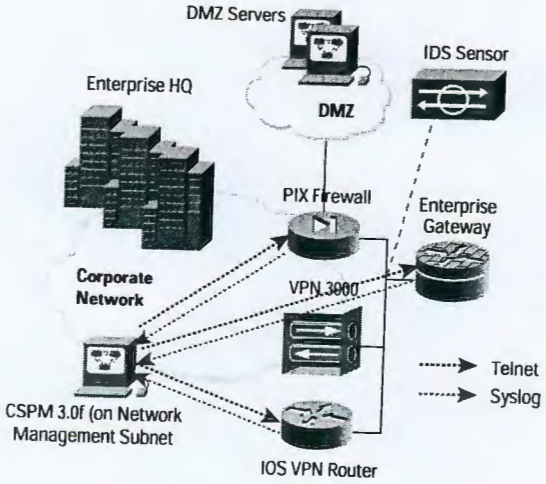
Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

44.634

Which services do I need to enable? (Application protocol requirements)

CSPM requires several protocols in order to function. First, when applying a security policy across the network, CSPM will use Telnet (TCP port 23) to connect to the device(s) and make configuration changes. The second protocol is syslog (UDP port 514). The CSPM has the ability to receive and consolidate syslog messages from the Cisco devices that it is managing. The application keeps an archive of these syslog messages and can use them to generate reports based upon the information they provide. Based on these requirements, the devices must then be configured to support these services. For both Cisco IOS Software and PIX, the telnet service along with a login password must be enabled. These devices also need to be configured to point their syslog messages to the CSPM server. Note that those devices managed by both RME and CSPM will now be sending their syslog messages to two different hosts. Figure 11 illustrates how CSPM is applied in our reference topology.

Figure 11
CSPM Applied



RQS nº 03/2005 - CN
CPMI - CORREIOS
0165
Fls. Nº
3690
Doc.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.633

Putting It All Together

Clearly, it is important to distinguish which components to use, determine where to deploy the various components of VMS, and identify what elements of the network infrastructure each piece manages. Table 12 summarizes the information presented in this section along with the associated management protocols that must be enabled in order for the applications to function properly.

Table 12 Summary of CiscoWorks VMS Components Applied

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

Caveats

When deploying VMS, it is important to realize the specific services required by each individual application, as outlined in the previous section. In certain instances, two different applications may require the same type of access to a particular device (for example, CiscoView and VPN Monitor both use SNMP to retrieve the management information). However, because some of the applications within VMS have a security focus, sharing access to a device can be a potentially contentious situation. This section discusses some of the things that need to be considered should you deviate from the deployment guidelines provided in this document.

Considerations with Network Address Translation

In many topologies, Network Address Translation (NAT) is used. This is an excellent feature for security and address space conservation, but it can create some problems with management tools. This section points out some of the caveats and issues that may occur if CiscoWorks VMS is deployed into a network environment with NAT.

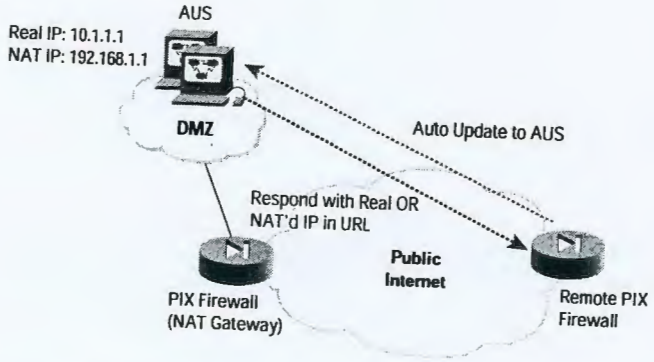
ROS nº 03/2003 - CN
CPMI - CORREIOS
0166
Fls. Nº
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

NAT and AUS

If the AUS application is used and the server is sitting behind a NAT gateway, pay special attention to the PIX Firewalls you are managing. Consider a remote PIX that contacts the AUS server. It will actually contact the NAT address (not the real address). When the AUS responds with the proper URL to download the updated configuration or software image, it will use the NAT address. Conversely, if the AUS is NOT behind a NAT gateway, you could also configure it to provide it's real address (Figure 12). The bottom line is that you have to decide to use the NAT address or the real address for ALL the PIX Firewalls you are managing—NAT and non-NAT addresses cannot be mixed within a single installation of AUS.

Figure 12
NAT and AUS



When it is necessary to manage PIX Firewalls (both internal and external), we recommend installing two copies of AUS—one for the external firewalls that will use the NAT address and one for the internal firewalls that will use the real IP address.

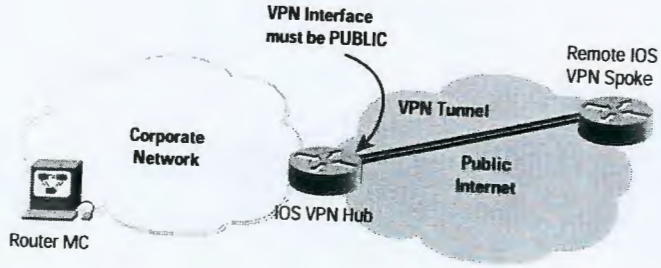
NAT and Router MC (Hub Side)

When using Router MC to set up a hub-and-spoke VPN environment, be careful about the hub router VPN interface. Because of the way the product is designed, this interface cannot be behind a NAT gateway. The VPN termination interface must be a publicly addressable IP subnet. If it was behind a NAT gateway, then from the perspective of the peer it would be necessary to assign it the NAT'd address. The Router MC application, however, only allows you to assign by interface and not IP address—so the peer statements will be incorrect. Refer to Figure 13 to see how the VPN topology must be built for compatibility with Router MC.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0167
Fls. Nº
Doc 3690

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 13
NAT and Router MC



NAT and Router MC (Spoke Side)

There is also a deployment caveat with NAT and VPN spoke devices. Router MC needs to manage the spoke devices (VPN peers) with their real IP address. The current version of Router MC does not support the situation where the spoke is behind a NAT gateway.

Managing a Device with CSPM and a MC

With the number of different applications within the VMS bundle, it is possible to have some functional overlap between tools. For example, if you want to change a PIX Firewall access rule, you can use either CSPM or PIX MC. This section describes some caveats and issues that exist when using overlapping applications.

CSPM and PIX MC

The first area of functional overlap is between CSPM and PIX MC. Both applications can be used to manage firewall device settings and access rules. So what happens when somebody tries to use both tools? Will this configuration even work?

The short answer is that this will NOT work. What will happen is when a configuration change is made using one of the applications, it will overwrite that change with the other application. This can be avoided by doing a re-import of the existing configuration before every deployment, but this is not practical. Also, you would need to make sure that you had an access rule set up to allow SSL traffic to the PIX. The recommendation here is to either use CSPM or PIX MC to manage a device, but not both.

CSPM and Router MC

The second area of functional overlap involves CSPM and Router MC. Both applications can be used to configure site-to-site VPNs on IOS VPN routers. CSPM can also be used to configure the firewall features set on those routers. Here, the consideration when each application would be used and how the two can work together.

As with PIX MC, avoid managing a single router's VPN settings with multiple applications. Even though Router MC does not push out a whole configuration file to the device (it sends out individual commands), it is possible that something will get overwritten in the original configuration. Looking at the reverse, it is definitely a problem if CSPM tries to configure a router that has already been configured with Router MC. The device will need to be re-imported into the CSPM database every time, just to make sure your configuration is current. This is also not very practical solution. Either use CSPM or Router MC to manage a device, but not both.

BOS nº 03/2003 - CN
CPMI - CORREIOS
Fls: 0168
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

34.630

When To Use What

Based on some of the overlap in product functionality, it can be confusing to decide which product should be used in what situations. CSPM is currently the only product that can help manage a mixed environment, so you need to use CSPM to set up a VPN tunnel between a PIX device and an IOS device. Otherwise, since they are designed for better scalability, it is ALWAYS recommended to use the MC applications instead, based on the network environment and management needs.

Multiple Syslog Daemons

Several applications within the VMS bundle can receive syslog messages from multiple sources. Now, with Cisco modified OS support, all of these applications can also be installed on a single server. In this case, it is necessary to determine how to make all of these syslog daemons compatible.

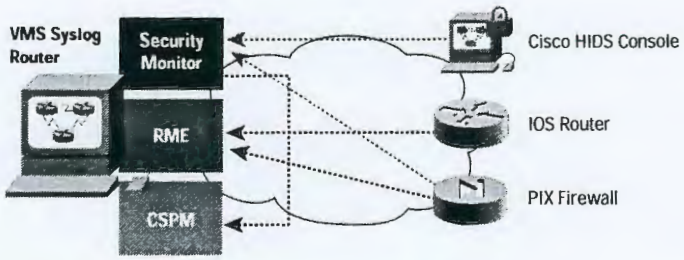
First, look at which applications can receive syslog messages, and from which devices (Table 13):

Table 13 Summary of Syslog Server Applications in VMS

CiscoWorks VMS Module	Syslog Source
RME	IOS, PIX, VPN3K
CSPM	IOS, PIX
Security Monitor	IOS, PIX, Host IDS Console

By default, all of these application listen on UDP port 514. This is not a problem if these applications are split across different servers—simply send syslog messages to multiple sources. However, what happens when all of these applications are installed on a single system AND the customer wants to try and take advantage of all three syslog daemons? (Figure 14.)

Figure 14
Syslog Consolidation in VMS



There are two ways that Security Monitor can alleviate this problem. The first is to configure what port number it should listen for syslog messages. By default it is UDP 514, but it can be changed. Also, Security Monitor can be set up to forward the syslog messages to another port on that same system. This is important because CSPM can change the port numbers they listen to for syslog messages. The other important factor is that PIX Firewalls can send syslog messages to the same host, but different port numbers. In this situation, here is the solution to maximize the syslog functionality:

CORREIOS
Fls. Nº 0169
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- From IOS, send syslog to RME at UDP 514
- From PIX, send syslog to RME at UDP 514
- From PIX, send syslog to Security Monitor at port x
- From Cisco HIDS Console, send syslog to Security Monitor at port x
- From Security Monitor, forward syslog to CSPM at port y

The only caveat here is that CSPM will not be able to receive IOS syslog messages.

Ideally, at least two servers would be used in this scenario to take advantage of all three tools. The first box would run Security Monitor and CSPM, and the second system would run RME. This way, no syslog functionality within VMS is lost.

Running the Cisco HIDS Software with other Applications

A major component of the CiscoWorks VMS bundle is the ability to manage IDS on a host level—or rather, to provide intrusion protection to critical servers. The management servers for VMS should definitely be considered critical and as such, we also recommend installing the Cisco HIDS agent software on these systems.

When installing another CiscoWorks VMS module on a server with Cisco HIDS, make sure the agent is in "Full Warning" mode during the install process. Running in "Full Protect" mode, it is possible that the normal operations of the software may trigger a HIDS event and, as such, may actually be prevented. In this case, a false positive would have an adverse effect on your management system by not allowing it to perform a legitimate task. In most cases, you should first install the Cisco HIDS agent and run it in "Full Warning" mode. Do this for the first several weeks of regular use to develop a baseline. This allows the user to first see events—but they will NOT be prevented. Based on this activity you can then identify any false positives and create appropriate exceptions. When the exceptions are configured, then you can change the status of your management server agents to "Full Protect" to ensure that the server is properly shielded.

Even using this deployment method, note that even in "Full Protect" mode out of the box, the HIDS agent software does not prevent any normal operations by any of the applications in the VMS bundle.

Compatibility Issues with IDS Event Viewer

Cisco IDS Event Viewer (IEV) is a Java-based application that lets users view and manage alarms from up to three IDS sensors. At the time of this writing, when IEV is installed on a PC, that PC can NOT be used as a client for the CiscoWorks VMS Web-based modules. While this compatibility limitation will be addressed in future releases, the current workarounds for this limitation are:

- Uninstall IEV from that client system
- Use a different PC as your client system

This will not be an issue for most users. Those using IDS MC and Security Monitor will most likely not need IEV as well.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0170
Doc. 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Out-of-Band Management

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices it is trying to manage. So when making this decision, consider that, while it might be nice to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

Conclusions

Evolution of VPNs and Security

In the recent past, we have seen huge growth in the need for network security, specifically in two areas: perimeter network security and secured transactions over public infrastructure. This growth has made it necessary to evolve how a management scheme handles this environment, which has resulted in the introduction of the CiscoWorks VPN/Security Management Solution (VMS).

The CiscoWorks VMS provides customers with applications to assist in the management of their security-specific hardware such as the Cisco VPN 3000 Concentrator series, Cisco IOS VPN routers, Cisco PIX Firewalls, and Cisco IDS products. VMS addresses the challenges of VPN deployment, monitoring, development of perimeter security policies, and management of intrusion detection. This paper provides some basic deployment guidelines for VMS by outlining the different components of the solution, what they do, and how they can be configured to work together. After reading this document, the user should clearly understand how VMS fits into the network management scheme and the values it adds.

As with any dynamic environment, the needs and technologies around network security are constantly evolving. From a network management perspective, CiscoWorks VMS will continue to evolve to provide a comprehensive set of tools to manage the unique aspects of this environment.

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

CORREIOS 0171 3690

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202881/ETMG 10/02

14.627
J

Switch Tipo 5 doc 10

RQS nº 03/2005 - CN
CPMI - CORREIOS
0172
Fls. Nº
3690
Doc.

Release Notes for VPN Client, Release 3.6.3.B

CCO Date: February 7, 2003

Part Number 78-15450-01

Note You can find the most current documentation for the VPN Client at http://www.cisco.com or http://cco.cisco.com. These electronic documents may contain updates and changes made after the hard copy documents were printed.

These release notes support VPN Client software Release 3.6 and all of its incremental "point" releases through Release 3.6.3.B. Please note that product release numbers are not necessarily consecutive. These release notes describe new features, limitations and restrictions, interoperability notes, caveats, and related documentation. Please read the release notes carefully prior to installation. A new section, "Usage Notes," describes interoperability considerations and other issues you should be aware of when installing and using the VPN Client.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003, Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0173
3690

Contents

Introduction, page 2
System Requirements, page 3
Installation Notes, page 4
New Features in Release 3.6.1 Through 3.6.3.B, page 8
Usage Notes, page 12
Open Caveats, page 27
Caveats Resolved in Release 3.6.3.B, page 40
Caveats Resolved in Release 3.6.3, page 44
Caveats Resolved in Release 3.6.2.B, page 44
Caveats Resolved in Release 3.6.2.A, page 45
Caveats Resolved in Release 3.6.2, page 46
Caveats Resolved in Release 3.6.1, page 47
Caveats Resolved in Release 3.6, page 48
Documentation Updates, page 56
Related Documentation, page 56
Obtaining Documentation, page 57
Obtaining Technical Assistance, page 58

Introduction

The VPN Client is a set of software applications that runs on a Microsoft® Windows®-based PC, a Sun ultraSPARC workstation, or a Macintosh personal computer that meets the system requirements stated in the next section. In this document, the term "PC" applies generically to all these computers, unless specified otherwise.

The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN).

CPMI - CORREIOS
0174
Fls. Nº
3690

System Requirements

Refer to Chapter 2, "Installing the VPN Client," in the *VPN Client User Guide for Windows, Release 3.6* or *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*, as appropriate for your platform, for a complete list of system requirements and installation instructions.

- To install the VPN Client on *any* system, you need
  - CD-ROM drive (if you are installing from CD-ROM)
  - Administrator privileges
- The following table indicates the system requirements to install the VPN Client on each of the supported platforms.

Computer	Operating System	Requirements
Computer with a Pentium®-class processor or greater	• Microsoft® Windows® 95 (OSR2), Windows 98, or Windows 98 (second edition) • Windows ME • Windows NT® 4.0 (with Service Pack 6, or higher) • Windows 2000 • Windows XP	• Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.) • 10 MB hard disk space. • RAM: – 16 MB for Windows 95/98 – 32 MB for Windows NT and Windows ME – 64 MB for Windows 2000 • 128 MB for Windows XP
Computer with and Intel x86 processor	RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later **Note** The VPN Client does not support Linux kernel Version 2.5.	• 32 MB Ram • 10 MB hard disk space

CPMI - CORREIOS
Fls. Nº 0175
3690

Computer	Operating System	Requirements
Sun UltraSPARC computer	32-bit or 64-bit Solaris kernel OS Version 2.6 or later	• 32 MB Ram • 10 MB hard disk space
Macintosh computer	OS X, Version 10.1.0 or later	5 MB hard disk space

The Cisco VPN Client supports the following Cisco VPN devices:

- Cisco VPN 3000 Concentrator Series, Version 3.0 and later.
- Cisco PIX Firewall, Version 6.1 (1) and later.
- Cisco IOS Routers, Version 12.2(8)T and later

Installation Notes

Because of platform differences, the installation instructions for Windows and non-Windows platforms also differ.

- Refer to the *VPN Client User Guide for Windows, Release 3.6,* Chapter 2, for complete installation instructions for Windows users.
- Refer to the *Cisco VPN Client user Guide for Linux, Solaris, and Mac OS X*, Chapter 2, for complete installation information for those platforms.

The following notes are important for users who are upgrading to Windows XP and users who want to downgrade to an earlier version of the VPN Client software.

Installation Changes - Windows Platforms

Release 3.6.x includes the following new installation changes for Windows users:

- The VPN Client no longer replaces the system GINA during the installation process. If you enable the "Start Before Logon" feature (available on Windows NT, Windows 2000, and Windows XP Professional Edition, but not on Windows XP Home Edition), the VPN Client automatically replaces and links to the original GINA.

RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 0176
3690

- Windows Installation Package (MSI) is now available for Windows NT (SP6), Windows 2000, and Windows XP.

Installing the VPN Client Software Using InstallShield

Installing the VPN Client software on Windows NT, Windows 2000, or Windows XP with InstallShield requires Administrator privileges. If you do not have Administrator privileges, you must have someone who has Administrator privileges install the product for you.

Installing the VPN Client Software Using the MSI Installer

If you are using the MSI installer, you must have Windows NT-based products such as Windows NT 4.0 (with SP6), Windows 2000, or Windows XP. Installing with MSI also requires Administrator privileges.

VPN Client Installation Using Windows Installer (MSI) Requires Windows NT SP6

When you attempt to install the VPN Client using MSI install (vpnclient_en.exe) on NT SP3, SP4, or SP5, the error messages do not indicate that the VPN Client cannot be installed on those operating systems because they are unsupported. Once the errors occur, no other messages are displayed and the installation is aborted.

When you attempt to run vpnclient_en.exe on Windows NT SP3, SP4, or SP5 you see the following messages:

"Cannot find the file instmsiw.exe (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."

-then-

"Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."

The Windows Installer (MSI) can be installed only on NT SP6, so the error messages you see using earlier service packs are due to an MSI incompatibility (CSCdy05049).

ROS nº 03/2005 - CN
CORREIOS
Fls Nº
3690

Close All VPN Client Applications Before Uninstalling the VPN Client.

If one of the VPN Client applications is running while the VPN Client is being uninstalled, a message box appears giving the following three choices: Cancel, Retry, Ignore.

If you select Ignore, the application continues running, but the VPN Client and all applications are uninstalled. When the computer reboots, the application is no longer on the hard drive (CSCdx42035).

Installation Notes - Solaris Platforms

The following sections describe actions you must take when installing the VPN Client on a Solaris platform.

Uninstall an Older VPN Client If Present on a Solaris Platform

If you have a previous version of the VPN Client running under Solaris, you *must* uninstall the older VPN Client before installing a new VPN Client. You are not required to uninstall an old VPN Client, if one is present, *before* installing a new VPN Client for Linux or Mac OS X.

Refer to the *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*, Chapter 2, for complete uninstallation information.

Disable the ipfilter Firewall Kernel Module Before Installing the VPN Client on a Solaris Platform

If you have an IP firewall installed on your workstation, the reboot after installation of the VPN Client takes an inordinate amount of time. This is caused by a conflict between the vpnclient kernel module cipsec and the ipfilter firewall module. To work around this issue, disable the ipfilter firewall kernel module before you install the VPN Client (CSCdw27781).

EPMI - CORREIOS
0178
Fls. Nº
3690

Using the VPN Client

- To use the VPN Client, you need
  - Direct network connection (cable or DSL modem and network adapter/interface card), or
  - Internal or external modem, and
  - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, www.microsoft.com. Windows 98 includes the DUN 1.3 function.)

Note The VPN Client may have data transfer problems if installed on a Windows 95a system. We recommend that you do not use the VPN Client on Windows 95a. If you must use Windows 95 instead of a more recent version, make sure that you are using Windows 95 OSR+.

To check the version of Windows you have, open the Control Panel | System | General tab and look for the System version. Windows 95a is: 4.00.950a (CSCdt07587)

- To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
  - Baltimore Technologies (www.baltimoretechnologies.com)
  - Entrust Technologies (www.entrust.com)
  - Netscape (www.netscape.com)
  - Verisign, Inc. (www.verisign.com)
  - Microsoft Certificate Services — Windows 2000
  - A digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

ROS [redacted]7 [redacted]5 - CN
CPMI - CORREIOS
Fls. Nº 0179
Doc. 3690

14.639
3

Windows XP Requires VPN Client Release 3.1 or Higher

If you are running Windows XP on your PC, you *must* upgrade your VPN Client to Release 3.1 or higher. VPN Client Release 3.0 does not support Windows XP.

If you are running the VPN Client on a PC and you want to upgrade your operating system to Windows XP, you must *first* uninstall the VPN Client, then install Windows XP, then install the VPN Client.

New Features in Release 3.6.1 Through 3.6.3.B

These release notes update the VPN Client to resolve several outstanding caveats. Refer to the appropriate "Caveats Resolved in Release 3.6.x" of these release notes for details on each release.

New Features in Release 3.6

Release 3.6 of the VPN Client software includes the following new features.

Dynamic DNS

The VPN Client sends its hostname to the VPN Concentrator during connection establishment. The VPN Concentrator can send the hostname in a DHCP request that can cause a DNS server to update its database to include the new hostname and Client address.

Split DNS

Release 3.6 has the ability to direct packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN Server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network.

ROS nº 03/2005 - CN
CPMI - CORREIOS
FIS Nº 0180
3690

For example, a query for a packet destined for *corporate.com* would go through the tunnel to the DNS that serves the private network, while a query to for a packet destined for *myfavoritesearch.com* would be handled by the ISP's DNS. This feature is configured on the VPN Server (VPN Concentrator) and enabled on the VPN Client by default.

AES (Existing DH Groups)

Advanced Encryption Standard is an encryption algorithm, recently approved by NIST, for securing sensitive but unclassified material by U.S. Government agencies. AES applies mostly to the VPN Concentrator, where new default IKE proposals and IPSec SAs have been added. The VPN Client can use AES in establishing remote access connections with the VPN Concentrator. On the VPN Client, AES shows up as an Encryption in use on connection status screens. We support AES-128 and AES-256 key sizes.

Note The VPN Client still supports DES/MD5; however, support for DES/SHA is no longer available. Because of the latter, Release 3.6 VPN Clients cannot connect to any central-site device group that is configured for (or proposing) DES/SHA. The VPN Client must either connect to a different group or the administrator for the central-site device must change the configuration from DES/SHA to DES/MD5 or another supported configuration. The *VPN Client Administrator Guide* lists all the supported encryption configurations.

Auto Initiation of VPN in a Wireless Environment

The Cisco VPN Client can be configured to automatically initiate a VPN based on the network that the user's machine is connected to (that is, based on a user's assigned address). This feature is called Auto Initiation for on-site Wireless LANs (WLANs).

The auto initiation feature was designed to make the user experience more like a traditional wired network in those environments in which VPNs are being used to secure WLANs. These environments are also known as on-site WLANs.

0181
Fls Nº
3690

NAT Traversal (NAT-T), Including Auto-detect

NAT-T lets the VPN Client and the VPN Concentrator automatically detect when to use IPSec over UDP to work properly in Port Address Translation environments. NAT-T is an IPSec Working Group draft: draft-ietf-ipsec-nat-t-ike-02. See the *VPN Client Administrator Guide*, Chapter 1, for instructions on how to configure this feature on the VPN Concentrator.

Update of Centrally-Controlled Backup Server List

VPN Client can learn the backup VPN Concentrator list during connection establishment. This feature is configured on the VPN 3000 Concentrator and pushed to the VPN Client. The addresses show in the VPN Dialer application in the Enable Backup Servers box under Options->Properties->Connections.

Peer Certificate Distinguished Name Field Verification

This feature prevents a client from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the Distinguished Name of the peer certificate fails, the client connection also fails. There is no user-visible change for this feature, but it requires a change to the connection profile.

CPMI - CORREIOS
Fls. Nº 0182
3690

New Global Profile Configuration Parameters (vpnclient.ini)

Release 3.6 adds the following new global profile configuration parameters under [Main]:

AutoInitiationEnable	Enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.
AutoInitiationRetryInterval	Specifies the number of minutes to wait before retrying an auto initiation connection. The range is 1 to 10 minutes. The default retry interval is one minute.
AutoInitiationList	Provides a series of section names, each of which contains a network address, a subnet mask, and a connection entry name. The network and subnet mask identify a subnet. The connection entry specifies a connection entry profile (.pcf file). You can include a maximum of 64 section (network) entries.

See the *VPN Client Administrator Guide, Release 3.6* for examples of using these parameters.

Creating Profiles for Client Users — New Parameters:

Release 3.6 adds the new keyword VerifyCertDN under [Main] for defining client profiles in the *.pcf file. This keyword prevents a user from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the Distinguished Name of the peer certificate fails, the client connection also fails.

Note In the *.pcf file, do not set the DHgroup parameter to 1.

11
CORREIOS
Fls. N° 0183
3690

New Parameters for Customizing the VPN Client Software

Release 3.6 adds new parameters to the oem.ini file for customizing the VPN Client software. For information about these parameters, see the *VPN Client Administrator Guide*, Chapter 5.

Stateful Firewall (Always On) Allows Inbound Tunneled Access

A Stateful Firewall (Always On) now allows inbound access from the internal (tunneled) network to ensure that system management applications work properly, while still providing additional protection by blocking all non-tunneled inbound traffic.

MSI - Microsoft Installer (Windows Installer) Support

MSI - Microsoft Installer (Windows Installer) package is now available for Windows NT, 2000, and XP. This package assists in packaging and customizable installation on these systems. This package is available in addition to the InstallShield installation package, which supports Windows desktop platforms.

Solaris 64-bit Support

The VPN Client now operates on Solaris UltraSPARC 64-bit systems.

Usage Notes

This section lists issues to consider before installing Releases 3.6 through 3.6.3 of the VPN Client software.

In addition, you should be aware of the open caveats regarding this release. Refer to "Open Caveats" on page 27 of these Release Notes for the list of known problems.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0184
Fls. Nº 78-15450-01
Doc. 3690

Potential Application Compatibility Issues

You might encounter the following compatibility issues when using the VPN Client with specific applications. Whenever possible, this list includes a description of the circumstances under which an issue might occur and workarounds for potential problems.

Windows Interoperability Issues

The following known issues might occur with the indicated Microsoft Windows operating systems and applications software.

WINS Support

On Windows 95 and Windows 98, dynamic WINS support works with DHCP-enabled adapters (for example, PPP or NIC adapters that get their IP information dynamically). For static configurations, users must manually configure the adapters with WINS information.

Windows NT

Users running Windows NT 4.0 with Service Pack 4 require a hot fix from Microsoft for proper operation. This fix is available on the Microsoft GetHostByName API Returns Unbindable Address page: http://support.microsoft.com/support/kb/articles/Q217/0/01.ASP.

Importing a Microsoft Certificate Using Windows NT SP3

The following problem has occurred on some Windows NT SP3 systems (CSCdt11315).

When using the Client with digital certificates stored in the Microsoft certificate store, the Client may fail to connect. This is accompanied by the following Client event in the Log Viewer:

4101 13:41:48.557 01/05/01 Sev=Warning/2 CERT/0xA3600002
Could not load certificate (null) from the store.

RDS nº 03/2005 - CN
CORREIOS
Fls Nº 0185
3690

Workaround: Two workarounds exist. Choose one of the following:

- Import the certificate from the Microsoft certificate store into the Cisco certificate store using the Cisco Certificate Manager. Refer to "Importing a Certificate" in the *VPN Client User Guide for Windows, Release 3.6*, Chapter 6.
- Alternatively, upgrade to a Windows Service Pack later than SP3.

VPN Client Cannot Launch Microsoft Connection Manager

The VPN Client does not see a dialup connection made with Microsoft Connection Manager because of incompatibilities between the requirements of the two applications (CSCdx85663).

Cannot Simultaneously Run the Cisco VPN Client and Windows 2000 Client

When switching between the Cisco VPN Client and the Windows 2000 L2TP/IPSec client, follow these steps (CSCdt84026):

Step 1 Stop the Cisco VPN service and driver. At the command prompt, enter:

```
net stop cvpnd
net stop cvpndrv
```

Step 2 Enable the MS IPSec service (IPSec Policy Agent) by entering:

```
net start policyagent
```

Windows 98 Might Hang on Shutdown

On some Windows 98 PCs with the VPN Client installed, if you restart the PC, it may stop responding (that is, "hang") on the screen that says "Windows is shutting down".

Wait a minute. If the PC is still not responding, press the reset button. When the PC reboots, it should not run through ScanDisk, indicating the shutdown was successful in closing all open files. This problem may occur on some PCs and not on others, and we are looking for a solution. Windows 98 shutdown has numerous issues, as can be seen the following Microsoft Knowledge Base Article:

"Q238096 - How to Troubleshoot Windows 98 Second Edition Shutdown Problems" (CSCdt00729).

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0186
3690
Doc.

Windows 2000 (only) Requires Adding Client for MS Networks for Dialup Connections

For the Cisco VPN Client running on a Windows 2000 system, you cannot access Microsoft resources unless you add the Client for Microsoft Networks for the Dial-up adapter.

Aladdin Runtime Environment (RTE) Issue with Windows NT and Windows 2000

Using versions of the Aladdin Runtime Environment (RTE) on Windows NT and Windows 2000 can cause the following behavior. The login prompt that is posted by the Aladdin etoken when connecting the VPN Client can get hidden in the background. If this happens, the VPN connection can timeout and fail with the following event:

"System Error: Connection Manager failed to respond."

A side effect of this is that the VPN Client's service and dialer might become out of synch, and the PC might need to be restarted (CSCdv47999). To avoid this issue, use the Aladdin Runtime Environment (RTE) version 2.65.

Microsoft MSN Installation

Microsoft's MSN installation fails if you have already installed the VPN Client. Uninstall the VPN Client before you install MSN. After MSN has completed installation, you can install the VPN Client.

VPN Client Might Not Be Removed from Windows Servers If Not Disconnected Before Shutdown

The VPN Client on Windows NT or Windows 2000 WINS servers may not be removed if the PC is shut down without disconnecting the VPN Client and the "Disconnect VPN connection when logging off" feature is disabled.

If the VPN Concentrator is configured to send WINS server addresses down to the VPN Client and the PC is shut down or restarted without first disconnecting the VPN Client, the WINS servers are not removed from the network properties. This might cause local PC registration and name resolution problems while not connected with VPN.

To work around this problem, do *one* of the following:

- Be sure to disconnect the VPN Client before shutting down. If you are having problems, check your network properties and remove the WINS entries if they are not the correct ones for your network.

15
CPMI - CORREIOS
Fls Nº 0187
3690

- Alternatively, enable "Disconnect VPN connection when logging off". Go to Options > Windows Logon Properties, check Disconnect VPN connection when logging off (CSCdv65165).

VPN Client May Falsely Trigger Auto Initiation Connection Event though the NIC Card Has Been Removed

The 3.6 VPN Client with Auto Initiation enabled on a Windows NT system may exhibit the following behavior. After removing a NIC card, the VPN Client may continue to trigger an Auto Initiation connection event though the NIC card has been removed. To stop its connection attempts, you can place the VPN Client in Suspended mode after a failed or canceled VPN connection. You can also disable this feature from the GUI by using Options > Automatic VPN Initiation, and unchecking "Enable". If you add a new NIC, the problem goes away. (CSCdx46812).

Allowing the VPN Client to Work Through ESP-Aware NAT/Firewalls

When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

To allow the VPN Client to work through ESP-aware NAT/Firewalls, add the following parameter and setting to the [Main] section of any *.pcf (profile configuration file) for the affected connection profile.

ForceKeepAlives=1

This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

For more information, see "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide, Release 3.6.*

DNS

For DNS resolution, if the DOMAIN NAME is not configured on the network interface, you need to enter the fully qualified domain name of the host that needs to be resolved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0188
3690

Network Interfaces

- The VPN Client cannot establish tunnels over Token Ring. However, it does not conflict with an installed Token Ring interface.
- DELL Docking Station users running the VPN Client on Windows NT may experience bluescreen failures if the latest version of Softex Docking Services has not been installed. The Softex Docking Service utilities are available directly from the DELL Support Web site, http://search.dell.com/index.asp. Select the checkbox for the File Library and search for the term "Softex Docking Services".

Network ICE BlackICE Defender Configuration

Network ICE's BlackICE Defender is a traffic monitoring security product. If you properly configure it, BlackICE Defender can work with the VPN Client. You must configure BlackICE Defender for Trusting, Nervous, or Cautious mode. If you use Nervous or Cautious mode, add the public IP address of the VPN Concentrator to the list of trusted addresses. You can now configure the VPN Client to work with BlackICE Defender configured for Paranoid mode when in Tunnel-everything mode. Split Tunneling requires BlackICE to be in Trusting, Nervous, or Cautious mode.

The Cisco VPN Client firewall has the following requirements for BlackICE (BlackICE Defender 2.5 or greater or BlackICE Agent 2.5 or greater). For BlackICE Defender 2.5, copy the BICTRL.DLL file from the Cisco installation release medium to the BlackICE installation directory on the VPN Client PC. This is a mandatory step for making a connection requiring BlackICE.

BlackICE Defender version 2.9 and greater includes the BICTRL.DLL file in the Network ICE distribution medium, so that you do not need to copy it from the Cisco installation release medium.

Microsoft Outlook Error Occurs on Connection or Disconnect

The following Microsoft Outlook error might occur when the VPN Client connects or disconnects:

"Either there is no default mail client, or the current mail client cannot fulfill the messaging request. Run Microsoft Outlook and set it as the default mail client."

17 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0189
3690

This message does not affect operation of the VPN Client. The issue occurs when Microsoft Outlook is installed but not configured for email, although it is the default mail client. It is caused by a Registry Key that is set when the user installs Outlook.

To eliminate this message, do one of the following:

- Right-click the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail as the default mail client.
- Use Internet Explorer to configure the system to have no default mail client.
- Configure Outlook as the default mail client (CSCdv67594).

Adjusting the Maximum Transmission Unit (MTU) Value

VPN Encapsulation adds to the overall message length. To avoid refragmentation of packets, the VPN Client must reduce the MTU settings. The default MTU adjusted value is 1300 for all adapters. If the default adjustments are not sufficient, you may experience problems sending and receiving data. To avoid fragmented packets, you can change the MTU size, usually to a lower value than the default. To change the MTU size, use the VPN Client SetMTU utility. If you are using PPPoE, you may also have to set the MTU in other locations. Refer to the following table for the specific procedures for each type of connection.

The MTU is the largest number of bytes a frame can carry, not counting the frame's header and trailer. A frame is a single unit of transportation on the Data Link Layer. It consists of header data, plus data that was passed down from the Network Layer, plus (sometimes) trailer data. An Ethernet frame has an MTU of 1500 bytes, but the actual size of the frame can be up to 1526 bytes (22-byte header, 4-byte CRC trailer).

Recognizing a Potential MTU Problem

If you can connect with the Cisco VPN Client but cannot send or receive data, this is likely an MTU problem. Common failure indications include the following:

- You can receive data, such as mail, but not send it.
- You can send small messages (about 10 lines), but larger ones time out.
- You cannot send attachments in email.

14.609
Fls 0190
3690

Setting the MTU Value

Usually, an MTU value of 1300 works. If it doesn't, the end user must decrease the value until the Cisco VPN Client passes data. Decrement the MaxFrameSize value by 50 or 100 until it works.

The following table shows how to set the MTU value for each type of connection.

Connection Type	Procedure
Physical Adapters	Use the SetMTU utility supplied with the Cisco VPN Client.
Dial-up	Use the SetMTU utility supplied with the Cisco VPN Client.
PPPoE - All Vendors	**Windows XP *only*** Use SetMTU
PPPoE - EnterNet	**Windows 9x** • On the main desktop, right click on My Network Places and go to Properties. The Network window opens. • Double-click the Network TeleSystems PPPoE Adapter. • On the Network TeleSystems window, click the Advanced tab, and then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 • On the main desktop, right-click My Network Places and go to Properties. The Network and Dial-Up Connections window opens. • Right-click and go to Properties on each connection until you find the connection that has the NTS EnterNet PPPoE Adapter. • Once you find the correct connection, click Configure on the right side of the window. • On the next window, click the Advanced tab, then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

RQS 19 05 - CN
CPMI - CORREIOS
Fls. Nº 0191
3690

Connection Type	Procedure
PPPoE - WinPoet	**Windows 9x:** WinPoet does not provide user control over the PPPoE MTU under Windows 9x. **Windows 2000** WinPoet does not provide a user interface to control the MTU size, but you can control it by explicitly setting the following registry key: HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber> adapter(000x): Value: MaxFrameSize Value type: DWORD Data: 1300 (or less) The GUID and adapter number can vary on different systems. Browse through the registry, looking for the MaxFrameSize value (CSCdu80463). ⚠ **Caution** Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable.
PPPoE - RasPPPoE	**Windows 9x** • On the main desktop, right-click My Network Places and go to Properties. The Network window opens. • Find the PPP over Ethernet Protocol that is bound to the Network card that is in your PC, then double click on it. • In the General Tab check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 • On the main desktop, right-click My Network Places and go to properties. The Network and Dial-Up Connections window opens. • Right-click the connection the PPPoE Protocol was installed to, and go to properties. • When the window opens, double-click PPP over Ethernet Protocol. • In the General Tab, check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0192
Fls. Nº
3690
Doc.

14.606
3

Asante FR3004 Cable/DSL Routers Require Asante Firmware Version 2.15 or Later

Versions of the Asante firmware caused a problem with rekeying and keepalives when a VPN Client had an all-or-nothing connection to a VPN Concentrator through an Asante FR3004 Cable/DSL router. Version 2.15 (or later) of the Asante firmware resolves these issues. For more information about Asante cable/DSL routers, see the following Web sites:

- http://www.asante.com/products/routers/index.html
- http://www.practicallynetworked.com/pg/router_guide_index.asp

Using Nexland Cable/DSL Routers for Multiple Client Connections

All Nexland Pro routers support passing multiple IPSec sessions through to Cisco VPN 3000 Series Concentrators. To enable this function, the Nexland user must select IPSec Type 2SPI-C on the Nexland options page.

The discontinued Nexland ISB2LAN product correctly handles a single connection, but problems can occur when attempting to make multiple client connections to the same Secure Gateway from behind an ISB2LAN Nexland Cable/DSL router. Nexland has fixed this problem in the Nexland Pro series of routers (CSCdt10266).

Cert DN Matching Cannot Match on Email Field EA

You cannot match on the Cert DN field (EA) when using the Peer Cert DN Verification feature because the VPN Concentrator does not assign a value to that field (CSCdx25994).

Long (over 200) Network List Might Cause Client Failure

If the VPN 3000 Concentrator is configured to send a network list containing 200 networks to the VPN Client, the VPN Client service might fail. To resolve this issue, reduce the number of networks in the network list, restart the client PC, and reconnect (CSCdt06772).

21
RQS - CN
CPMI - CORREIOS
Fls. Nº 0193
3690

14.605

VPN Dialer Application Can Load During OS Shutdown or Restart

When using the VPN Client's Start Before Logon feature (Windows NT, Windows 2000, or Windows XP) in "fallback" mode, the VPN dialer application loads during a shutdown or restart of the operating system. This will not cause any problems and can be ignored (CSCdu02071).

America Online Users (AOL) Versions 5.0 and 6.0

The VPN Client supports AOL Version 5.0. AOL Version 6.0 is also supported, with one limitation: when connected, browsing in the network neighborhood is not available.

America Online Users (AOL) Version 7.0

AOL Version 7.0 uses a proprietary heartbeat polling of connected clients. This requires the use of split tunneling to support the polling mechanism. Without split tunneling, AOL disconnects after a period of time between 5 and 30 minutes.

Browser Interoperability Issues

The following known issues might occur when using the VPN Client with the indicated browser software.

Issues Loading Digital Certificate from Microsoft Certificate Store on Windows NT SP5 and on IE 4.0 SP2

The following error occurs in the VPN Client log when using a Digital Certificate from the Microsoft Certificate Store. This can occur on Windows NT 4.0 with Service Pack 5 and on Internet Explorer 4.0 with SP2 and using the VPN Client v3.1 or v3.5:

"Could not load certificate cn=Joe Smith,ou=Engineering,o=MyCompany,l=Buffalo, st=new york,c=US,e=jsmith@mycompany.com from the Unsupported Store store"

Both the VPN Client and the Certificate Manager can see and validate the Certificate, but when you try to connect using that Certificate, you get a message in the Connection History dialog that says, "Failed to establish a secure connection to the security gateway".

ROS nº 03/2005 - CN
CPMI - CORREIOS
0154
Fls Nº
3690

14.604

To fix this problem, do *one* of the following:

- Upgrade to Internet Explorer v5.0 or greater.
- Upgrade the PC to Service Pack 6.0a (CSCdv70215).

Cannot Connect 3.6 VPN Client for Windows Using Digital Certificate With Non-exportable Keys

A PC must have Internet Explorer version 5.0 SP2 or later installed to function properly using certificates with non-exportable keys (CSCdx90228).

Entrust Entelligence Issues

The following known issues might occur when using Entrust Entelligence software with the VPN Client.

Potential Connection Delay

Using the VPN Client with Entrust Entelligence might result in a delay of approximately 30 seconds if you are trying to connect while Entrust is "online" with the CA. This delay varies, depending on your Entrust CA configuration. If the Entrust CA is on the private network, then the chance of Entrust being online are low, since the VPN connection is needed to communicate with the CA.

If you experience this delay, do *one* of the following:

- Wait for the delay to end and proceed with the VPN connection normally.
- Before initiating the VPN Client connection, log out of Entrust. The VPN Client will initiate the Entrust Login Interface with the "work offline" checkbox checked, which alleviates the problem. The easiest way to log out of Entrust is to right-click on the Entrust tray icon (gold key) and select "Log out of Entrust" (CSCdu25495).

Entrust System Tray Icon Might Erroneously Indicate Logout

When using VPN Client with Start Before Logon (Windows NT and 2000) and Entrust Entelligence, the Entrust system tray icon indicates that it is "logged out" once in Windows. It is really logged in, just not in the normal Windows desktop. The reason for this is that the context that Entrust was logged into was on the "Logon desktop". This is an Entrust issue, not a VPN Client problem.

Entrust operates normally once logged into within Windows (CSCdu29239).

ROS nº 03/2005 - CN - CORREIOS
Fls. Nº 0195
3690

Entrust Client May Appear Offline

After establishing a VPN connection with Entrust Entelligence certificates, the Entrust client may appear offline. It may appear this way even after the Entrust client has successfully communicated with the Entrust i500 directory.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Once connected, right click on the Entrust tray icon (gold key) and uncheck "Work Offline". This manually puts Entrust online (CSCdu33638).

Use Entrust Entelligence 4.0 with VPN Client Release 3.5.1 or 3.1 Start Before Logon

When using the Release 3.5.1 or 3.1 VPN Client with the Entrust Entelligence 4.0 software, the Start Before Logon feature does not function properly. Upgrading to Entrust Entelligence 5.1 resolves this problem (CSCdu61926).

Some Entrust Dialogs Do Not Display Properly When Using VPN Client Start Before Logon

When using the VPN Client with Start Before Logon and Entrust Entelligence, some Entrust dialogs do not display properly on the logon desktop that displays before going into Windows NT or Windows 2000. The first time the VPN Client dialer and service access the Entrust certificates, it prompts for a security check. This prompt displays in Windows, but not at the logon screen.

To work around this problem, connect the VPN Client once, while in Windows and after installing, to register the VPN applications (ipsecdialer.exe and cvpnd.exe) with Entrust. Once you have done this you can use it at the logon desktop (CSCdu62212).

Renewing Entrust Entelligence Certificate (Key Update) Requires Entrust Version 5.1 SP 3 or Later

Entrust Entelligence certificate renewal (key update) will not work over a VPN Client connection unless Entrust Entelligence version 5.1 SP3 or later is being used. Other Entrust Entelligence operations using older versions work properly.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Computers need to have Entrust digital certificates renewed by placing them directly on the network during the renewal period to get updated (CSCdu84038).

RQS nº 03/2005 - CN
CPMI - CORREIOS
0196
3690

J4.602

Manual Reboot Required after Automatic Uninstall of Nortel VPN Client

If the Nortel VPN Client version 2.51 is upgraded to version 2.62, the Cisco VPN Client detects and offers to uninstall the Nortel Client. After the uninstall completes, the user must manually reboot the PC. Setup does not automatically offer to do the reboot (CSCdu30079).

Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

"The page cannot be displayed."

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

ZoneAlarm Plus Versions 3.1.274 and Earlier Are Incompatible with VPN Client

The following known incompatibility exists between the Cisco VPN Client and Zone Labs ZoneAlarm Plus version 3.1.274 and earlier. If you are using such a version of ZoneAlarm Plus, please visit http://www.zonelabs.com or contact your Zone Labs representative for an update.

On a PC with ZoneAlarm Plus version 3.1.274 (or earlier) and the VPN Client, the following errors occur when the PC boots:

On Windows 2000:

> ZAPLUS.exe has generated errors and will be closed by Windows. You will need to restart the program.
>
> An error log is being generated.

The Application Log states:

> The application, ZAPLUS.EXE, generated an application error. The error occurred on 7/23/2002... The exception was c0000005 at address 00401881 (<nosymbols>).

Similar errors occur on other Windows operating systems.

25 03/2005 - CN
CPMI - CORREIOS
FIs. Nº 0197
3690

The result of this error is that the ZoneAlarm GUI does not run, and therefore a user can not change any settings in ZoneAlarm Plus or allow new programs to access the Internet.(CSCdy16607).

CVPND Listens on UDP Port 500 When Not Connected

When the VPN Client is installed, you will find it is LISTENING on UDP Port 500, which is used for IKE negotiation. Even though the port is in a LISTENING state, the VPN Client cannot accept incoming connection attempts from other IPSec Clients or devices.

The port is in a LISTENING state because the VPN service is started at boot time. This service may take up to 10 seconds to start and if the service was started at connect time, each connection attempt would take an additional 10 seconds to complete. Always having the service running makes call setup time quick for our customers (CSCdt41339).

Harmless Warning Might Occur with Linux Kernel 2.4

Linux users running 2.4 kernels may encounter the following warning when the VPN Client kernel module is loaded:

> Warning: loading /lib/modules/2.4.18-3/CiscoVPN/cisco_ipsec will taint the kernel: no license

This message indicates that the VPN Client kernel module is not licensed under the GPL, so the Linux kernel developers will not debug any kernel problems that occur while this kernel module is loaded. This message does not affect the operation of the VPN Client in any way (CSCdy31826).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0198
3690

Open Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following lists are sorted by platform and then by identifier number for the specified platform.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats for the VPN Client on Windows Systems

This section lists open caveats for the VPN Client running on a Windows platform.

- CSCdt07491

  The VPN Client may swap Primary and Secondary WINS received from the Concentrator. In a few cases, the VPN Client receives a Primary and a Secondary WINS server from the Concentrator but swaps them when they are added to the IP Configuration. If this happens, it may cause browsing problems if the Secondary WINS server is not as populated as the Primary. Disconnecting and reconnecting may fix the problem.

- CSCdt07673

  When the VPN Client is installed on a Windows 2000 PC with the Efficient Networks NTS EnterNet 300 PPPoE version 1.41, the following message appears:

  "EnterNet could not find the (adapter) for complete pc management NIC (adapter). But it did locate the (adapter) for complete pc management NIC (adapter) - Deterministic Network Enhancer Miniport adapter through which your network server is reachable. Do you want to switch to this adapter?"

  Answer Yes every time this question appears. The installation then continues normally.

27 CPMI CORRE 0199 3690

A similar message appears on Windows NT 4.0. The message is:

"EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No"

Answer Yes to this question. The installation then continues normally.

If the VPN Client is uninstalled, the next time the NTS EnterNet 300 PPPoE version 1.41 is used the message, "EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No"

Answer Yes to this question. The installation then continues normally.

- CSCdt07787

  Problems have occurred when an ISA legacy NIC card (IBM Etherjet 10MB) is used in a PC with PnP OS enabled. The WINS servers did not function correctly when a VPN Client connection was made. This could be an issue with other legacy NIC cards as well.

  The end results are that the WINS servers sent from the Secure Gateway cannot be viewed in the Network configuration, and problems with browsing/logon over the VPN connection may occur.

  Workaround:

  Disable PnP OS in the PC's BIOS or statically configure the WINS servers.

- CSCdt13380

  When you connect the VPN Client to a VPN 3000 Concentrator that issues two DNS servers, both appear under ipconfig /all, but only one appears under the Network settings TCP/IP Properties. DNS server appears to be missing under TCP/IP Properties (Advanced button, DNS TAB). We do not know whether this causes any problems.

- CSCdt13398

  During a split-tunnel VPN Client connection, the first packets that bring up a new IKE SA may be lost. You may need to reconnect or relaunch network applications that do not automatically try to reconnect on their own.

- CSCdt41308

  You may see a problem with FTP file transfers over a long period of time (hours) while connected with the VPN Client. The symptom is that the FTP session never starts (no response to the 'open' command) and the Client Log Viewer shows the following events:

Fls. Nº 0200
3690

74 22:31:08.704 02/08/01 Sev=Warning/2 IPSEC/0xE370000C
Failed to acquire a TCP control resource, the queue is empty.

75 22:31:08.704 02/08/01 Sev=Warning/2 IPSEC/0xA370001A
VRS processing failed, discarding packet

Other applications like PING and HTTP should work fine, but for FTP to work again, you must disconnect and reconnect the VPN Client.

- CSCdt42661

  When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

  See the description of "Allowing the VPN Client to Work Through ESP-Aware NAT/Firewalls" on page 16 in these Release Notes for more information. Refer to "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide* for a detailed description of creating profiles.

- CSCdt56343

  You might see the following problem on systems running Windows NT and Windows 2000 when you are using the Start Before Logon feature of the VPN Client with third-party dialer. If the third-party dialer does not get set to the foreground when launched, add the following parameter to the vpnclient.ini file in the VPN Client directory (\Program Files\Cisco Systems\VPN Client\Profiles):

  [main]
  TopMostDelay=2500

  The value is the time in milliseconds that the VPN Client waits for the third party dialer to load before attempting to place it in the foreground. The default time is 1000 milliseconds.

  Workaround:

  For problem dialers/applications, try 2500 milliseconds or greater.

- CSCdu22174

  SCEP enrollment might fail to complete successfully after the PKI administrator has granted your request.

29 005 - CN
CPMI - CORREIOS
Fls. Nº 0201
3690

Workaround:

If this happens, delete your failed request and submit a new one.

To delete the request, open the Certificate Manager. Click the Enrollment Requests tab, and highlight the failed request. Select Options and delete.

- CSCdu50445

  The following issue can exist when using the VPN Client Start Before Logon feature with Entrust SignOn. Entrust SignOn is an add-on to the Entrust Entelligence client that allows logging into the Entrust profile and the NT domain from a single login.

  The Entrust SignOn GINA dll does not support chaining to other GINA dll files. To make the Entrust SignOn product and the VPN Client with Start Before Logon function properly together, install the VPN Client after Entrust SignOn. The VPN Client replaces the Entrust GINA (etabcgin.dll) with its own (csgina.dll).

- CSCdu62275

  VPN Client and Entrust Entelligence - VPN Connection Manager timeout.

  The potential exists for the VPN Client Connection Manager and the VPN Dialer to get out of sync with each other. This occurs only after a VPN Client upgrade on the first time the VPN Client accesses a given Entrust profile. The following sequence outlines how a user could get the connection into this state:

Step 1 In the VPN dialer, the user clicks Connect.

Step 2 Entrust prompts for password and security hash check. The user clicks Yes.

Step 3 Entrust prompts for password for cvpnd.exe security access.

If the user waits here or walks away from PC, the Connection Manager times out in 3 minutes.

Step 4 The user returns and enters the Entrust password, then clicks Yes to the security hash check question.

Step 5 The VPN connection completes, and data can be passed. The VPN dialer appears as not connected.

Step 6 Clicking Connect returns "A connection already exists". The user clicks Cancel, and the dialer appears connected in the system tray.

14.597
RQS nº 03/2005 - CN
CPMI - CORREIOS
0202
Fls. Nº
3690
Doc.

14.596

The VPN connection can be used as a normal connection.

- CSCdu70660

  This issue occurs on a Windows NT PC that is running ZoneAlarm, if the VPN Client is set to Start Before Logon and an upgrade to the VPN Client is implemented. Do not attempt a connection before the logon when you reboot, because ZoneAlarm does not automatically give the VPN Client permission to access the Internet. ZoneAlarm sees the upgrade as a new application attempting to access the Internet, and it requires user permission through its pop-up menus. The user must logon to the Windows NT PC using cached credentials, then launch a VPN connection. ZoneAlarm then asks permission to allow the VPN Client to connect. Answer yes to each connection. After that, Start Before Logon works fine.

- CSCdu77405

  The message, "The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server." might appear on a PC when Start Before Logon is enabled on the Client and ZoneAlarm is also running. The message appears when the ctrl+alt+del key combination is pressed. This has happened because the Cisco Systems VPN Service has terminated unexpectedly.

  Workaround:

  Logon to the PC with cached credentials, open "Services" in control panel and start the VPN service. A connection to the VPN Concentrator will be possible once the service has started.

- CSCdu81905

  When connecting to a VPN 3000 Concentrator over PPPoE using the EnterNet 300 client software from Efficient Networks, Inc., if a firewall is required by the VPN Concentrator, the following message might appear:

  "The Client did not match any of the Concentrator's firewall configurations..."

  If this message appears, click OK and then click Connect. The connection to the VPN Concentrator then proceeds successfully.

RQS [redacted] - CN
CPMI CORREIOS
0203
Fls. Nº
3690

J4.595

- CSCdu83054

  If you make connections from the command line interface using the NoTrayIcon parameter, the following problem can occur. When a firewall is required to connect and the firewall fails or is shut down, you do not see any message giving the reason for the lost connection.

- CSCdu86399

  If you use the VPN Client with a Digital Certificate and your Client sits behind a Cable/DSL router or some other NAT device, you might not be able to connect to your VPN Gateway device (that is, the VPN 3000 Concentrator). The problem is not with the VPN Client or the Gateway; it is with the Cable/DSL router. When the VPN Client uses a Digital Certificate, it sends the Certificate to the VPN Gateway. Most of the time, the packet with the Certificate is too big for a standard Ethernet frame (1500), so it is fragmented. Many Cable/DSL routers do not transmit fragmented packets, so the connection negotiation fails (IKE negotiation).

  This problem might *not* occur if the Digital Certificate you are using is small enough, but this is only in rare cases. This fragmentation problem happens with the D-Link DI-704 and many other Cable/DSL routers on the market. We have been in contact with a few of these vendors to try to resolve the issue.

  Testing with the VPN Client Release 3.1 indicates that VPN Client connections using Digital Certificates *can* be made using the following Cable/DSL routers with the following firmware:

Linksys BEFSRxx	v1.39 or v1.40.1
SMC 7004BR Barricade	R1.93e
Nexland Pro400	V1 Rel 3M
NetGear RT314	V3.24(CA.0)
Asante FR3004	V2.15 or later

  Others like 3COM 3C510, and D-Link DI-704 either had updated firmware that was tested and failed, or had Beta firmware that was NOT tested because the firmware notes did not indicate a fix specifically for fragmentation.

- CSCdu87521

  The following message might appear when a connection using the EnterNet 300 version 1.4 PPPoE software and transferring via FTP:

ROS nº 03/2005 - CPMI - CORRE
0204
Fls. Nº
3690

Jul. 594

93 09:42:06.020 08/02/01 Sev=Warning/2 IPSEC/0xE3700002
Function CniInjectSend() failed with an error code of 0xe4510000
(IPSecDrvCB:517)

This does not interfere with your connection. You can ignore this message.

- CSCdv40009

  When Zone Alarm's Internet setting is set to high and the VPN Concentrator sends a CPP firewall policy that allows inbound traffic on a specific port, the CPP rule takes precedence over the Zone Alarm rule allowing the specified port to be open.

- CSCdv42414

  Importing a PKCS12 (*.p12 or *.pfx) certificate using the Certificate Manager that has not been password protected will fail with the following error:

  "Please make sure your import password and your certificate protection password (if for file based enrollment) are correct and try again."

  Workaround:

  Get a *.p12 certificate that has been password protected.

- CSCdv43347

  If the Cisco VPN Client is not connecting when configured for digital certificates, the problem may not be indicated on the VPN Client connection history dialog. It may be helpful to run the Log Viewer application to see if any events are being displayed. To load it, click on the following and retry the connection.

  Start->Programs->Cisco Systems->VPN Client->Log Viewer

- CSCdv44529

  Attempting to install/uninstall Gemplus Workstation version 2.x or earlier while the Cisco VPN Client and its GINA (csgina.dll) is installed will cause the following error, and Gemplus will not install/uninstall:

  "A 3rd party GINA has been detected on your system. Please uninstall it before installing this product."

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0205
3690
Doc.

14.593

Workaround:

Do *one* of the following:

- Uninstall the VPN Client and reinstall it after Gemplus software.

or

- Use Gemplus version 3.0.30 that no longer installs the gemgina.dll

- CSCdv46591

  When a CPP Firewall policy is in place that drops all inbound and outbound traffic and no WINS address is sent to the VPN Client from the 3000 series Concentrator, Start Before Logon fails. If a WINS address is in place, Start Before Logon works fine. Also, if a WINS address is sent and the CPP rule drops all inbound traffic, but allows all outbound traffic, Start Before Logon works fine.

- CSCdv46937

  Using the Aladdin "R2" model etoken, certain functions can be performed using the certificate even after the R2 token has been detached from the system (USB port). The VPN Client, for instance, can perform an IKE rekey without the token attached to the system. The reason for this is the design of the "R2" etoken: it does not contain the RSA key functions needed and must upload the private key to the system for these functions.

  In contrast, the Aladdin "PRO" etoken must be connected to the USB port during an IKE rekey, otherwise the VPN Client connection terminates. This is Aladdin's problem; it is not a VPN Client problem.

- CSCdv62613

  When you have multiple VPN Client connections behind Linksys Cable/DSL router, the following problem can occur. Due to a Linksys problem with firmware versions 1.39 and 1.40.1, making multiple VPN Client connections enabling the feature "Allow IPSec over UDP" (transparent tunneling) may cause data transfer problems.

  Allow IPSec over UDP is a VPN Client feature that allows ESP packets to be encapsulated in UDP packets so they traverse firewall and NAT/PAT devices. Some or all of the clients may not be able to send data. This is due to a Linksys port mapping problem, that Linksys has been notified of.

DOC nº 08/2005 - CN
CPMI - CORREIOS
0206
Fls. Nº
3690

14.592

Workaround:

If possible, do not use the "Allow IPSec over UDP" (transparent tunneling) feature when you have multiple VPN Client connections behind Linksys Cable/DSL router.

- CSCdv67594

  The following Microsoft Outlook error might occur when the VPN Client connects or disconnects. This occurs when Microsoft Outlook is installed but not configured.

  In Microsoft Outlook, either there is no default mail client or the current mail client cannot fulfill the messaging request. Run Microsoft Outlook and set it as the default mail client.

  To do this, right-click on the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail.

- CSCdv85740

  Using BlackICE Defender version 2.9 with Windows 95 might cause a reboot or a blue screen after the connection to the Concentrator has been active for a period of time. This is a problem with NetworkICE, not the VPN Client.

- CSCdw60866

  Getting Entrust certificates using SCEP does not get the Root CA certificate. The Entrust CA does not send the whole certificate chain when enrolling with SCEP. Therefore, making a VPN Client connection might require the manual installation of the Root certificate before or after SCEP enrollment. Without the existence of the Root CA certificate, the VPN Client fails to validate the certificate and fails with the following VPN Client event/error messages:

  "Get certificate validity failed"
  "System Error: Unable to perform validation of certificate <certificate_name>."

- CSCdw73886

  If an attempt to load the VPN Client is made before the Clients Service loads, the following error occurs: "The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server."

  Workaround:

  Wait until the Service has loaded, then start the VPN Client.

CPMI - CORREIOS
Fls Nº 0207
3690

- CSCdx45719

  Downgrading the Cisco VPN Client from 3.6 to 3.5 and using the Start Before Logon feature results in the Start Before Logon running in fallback mode. This is due to some enhancements made to the csgina.dll file in 3.6 that the 3.5 VPN Client does not implement.

  Workaround:

  If downgrading and Start Before Logon are necessary, manually remove the VPN Client and then delete the csgina.dll file in the systems directory (usually c:\winnt\system32). This allows the 3.5 VPN Client to install its own csgina.dll file and operate normally.

- CSCdx51632

  If the computer is powered off or loses power during an MSI installation of the VPN Client, the VPN Client may not be registered in Control Panel, and the following may occur when attempting to reinstall:

  - A message may appear stating:
    Deterministic Network Enhancer Add Plugin Failed
    Click the "OK" button.
  - Error 1722. There is a problem with this Windows Installer package. A program as part of the setup did not finish as expected. Contact your Support personnel or package vendor. Click the "OK" button.
  - Error 1101. Error reading from file c:\config.msi\laff4.rbs. Verify that the file exits and you can access it. Click the "OK" button.
  - Error 1712. One or more of the files required to restore your computer to its previous state could not be found. Restoration is not possible. Click the "OK" button.

  After clearing the last message box, restart MSI installation. It should successfully install the VPN Client.

- CSCdx72463

  Installing the VPN Client using the Microsoft Windows Installer (MSI) displays "Time Remaining" for the installation. This time is not very accurate and should be ignored.

- CSCdx77292

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0208
Doc. 3690

14.590

Microsoft article Q234859 states that for the resiliency feature to work on Windows 4.0, IE 4.01 sp1 and shell32.dll version 4.72.3110.0 or greater must be installed on the computer.

- CSCdx78868

  The Microsoft Installer (MSI) resiliency (self healing) feature does not restore all files that are installed with the VPN Client. The files that will be restored are files that are associated with the shortcuts under Start | Program Files | Cisco Systems VPN Client.

- CSCdx81491

  An issue can occur when using the 3.6 VPN Client with Start Before Logon (SBL), after enabling SBL. The first time you log out of Windows, the VPN Client does not load after you press the CTRL+ALT+DEL key combination at the Windows logon prompt.

  Workaround

  Reboot the PC after enabling Start Before Logon; after a subsequent logout, the VPN Client should operate properly.

- CSCdx83687

  The following error occurs after the resiliency feature has reinstalled a missing file on Windows NT 4.0:

  c:\winnt\profiles\all users\start menu\programs\cisco systems vpnclient\xxx.lnk

  The Windows installer failed to install the program associated with this file.

  Please contact your system administrator.

  xxx.lnk is whatever file is being restored.

  When you click OK, the PC reboots and the file *is* restored. The resiliency feature is working, but the error should not appear.

- CSCdx88063

  When attempting to launch the dialer when the dialer is already running on the logon desktop (due to SBL or SBL and AI), the following error occurs instead of the VPN Client dialer loading.

  "Single dialer instance event creation failed with error 5."

  This is most likely to happen when Start Before Logon and Auto Initiate are being used on a Windows NT/2000/XP system.

RQS nº 03/2005 - CN
GPMI - CORREIOS
0209
Fls. Nº
3690
Doc.

Workaround

This is due to the fact that the VPN Client dialer is already running on the "logon desktop". Most likely during Windows logon the dialer launched and posted an error, the Windows logon was completed and the error was never closed. To work around this error, do the following:

Step 1 Press CTRL+ALT+DEL to get to the logon desktop.

Step 2 Look for and close any VPN Client error dialogs.

Step 3 Press ESC to return to the normal Windows desktop; the VPN Client should load normally.

- CSCdx89940

  A Restricted, Standard, or Limited user (Windows 2000) cannot install the VPN Client using the Windows Installer (MSI), even if elevated privileges are set for the user and the PC.

- CSCdy13425

  Connecting the Cisco VPN Client (versions 3.5 and later) to an IOS VPN device running 12.2(8)T using digital certificates might disconnect during a rekey. The connection could disconnect sooner if dead peer detection (DPD) is being used. The problem is under investigation.

  Workaround:

  Keeping the rekey times as high as possible will help avoid the problem.

  The other alternative is to use the VPN Client with preshared keys, which does not have the problem.

- CSCdy14218

  During installation of the VPN Client on a PC that already has the Enternet v.1.5c or v. 1.5c SP2, the following error might appear:

  "SVCHOST.EXE has generated errors and will be closed by Windows."

  Workaround:

  If this message appears, click OK, then reboot the PC when the VPN Client prompts for the reboot. After this, The message does not reappear and all connections work fine.

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-15460-01
0210
Fls Nº
3690
Doc

- CSCdy47745

  In the following specific case, the VPN Client fails to sent its IKE Keepalives (DPD - Dead Peer Detection) and then disconnect after the VPN Concentrator has been rebooted. This occurs only in the case where the VPN Client has been receiving the following Events in its log (also see CSCdt41308):

```
421    12:32:17.981  08/28/02  Sev=Warning/2 IPSEC/0xA3700019
VRS processing failed, discarding packet

422    12:32:19.984  08/28/02  Sev=Warning/2 IPSEC/0xE370000B
Failed to acquire a TCP control resource, the queue is empty.
```

Open Caveat for Linux

This section lists the open caveat for the VPN Client running on a Linux platform.

- CSCdv73541

  The make module process fails during installation of the VPN Client.

  Workaround:

  The module build process must use the same configuration information as your running kernel. To work around this problem, do one of the following:

  - If you are running the kernels from Red Hat, you must install the corresponding kernel-sources rpm. On a Red Hat system with kernel-sources installed, there is a symlink from /lib/modules/2.4.2-2/build to the source directory. The VPN Client looks for this link first, and it should appear as the default value at the kernel source prompt.
  - If you are running your own kernel, you must use the build tree from the running kernel to build the VPN Client. Merely unpacking the source code for the version of the kernel you are running is insufficient.

Open Caveat for Solaris

This section lists the open caveat for the VPN Client running on a Solaris platform.

- CSCdv75825

RQS nº 03/2005 - CN
CPMI - CORREIOS
0211
Fls Nº
3690
Doc:

If the VPN Client uses routed RIP to learn its default route, you might lose connectivity. This is because RIP is blocked when the VPN Client is connected in all tunneling mode.

Open Caveats for Mac OS X

There are no open caveats for the VPN Client running on Mac OS X.

Caveats Resolved in Release 3.6.3.B

- CSCdv43347

  If the Cisco VPN Client is not connecting when configured for digital certificates, the problem may not be indicated on the client connection history dialog. It may be helpful to run the Log Viewer application to see if any events are being displayed. To load it, retry the connection by clicking the following path:

  Start > Programs > Cisco Systems > VPN Client > Log Viewer

- CSCdw61796

  The Cisco VPN Client fails to connect while configured for digital certificates and posts the following error in the Log Viewer:

  "Get certificate validity failed".

  Some of the reasons this event could have occurred should be posted to Connection Status dialog and the Log Viewer. We notify the user with the following errors:

  - The certificate has an incomplete chain.
  - The certificate it either expired or not valid yet.
  - Certificates private key could not be opened.
  - Certificate signature was invalid.
  - User Certificate was not found.
  - Out of memory

RQS nº 03/2005 - CN
CPMI - CORREIOS
0212
78-15450-01
Fls. Nº
3690

14.586

- CSCdx54679

  When a Cisco VPN Connection is not established, users can't get to servers on the private network. But the Novell client caches these negative responses for performance reasons. But when a VPN Connection comes up, Novell client does not know that it can now reach the private servers, and fails the attempt to reach the private server (based on its cache). This can take users up to 5 minutes to reach the private Novell servers.

  For Novell client symptoms, see:

  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068795.htm.

  To avoid this problem, the Cisco VPN Client notifies the Novell driver after the VPN Connection comes up. Novell then clears its cache as a result of this notification. To avoid synchronization issues, we only notify the Novell client 5 seconds after the VPN Tunnel has come up.

- CSCdy50212

  When PC with VPN Client, Release 3.6 has the outside interface of the concentrator as its default gateway, the default gateway will be removed out of the windows routing table when the client disconnects. This has been seen only with non-English versions of Windows 2000 Professional and Windows 98SE.

- CSCdy81064

  When the adapter address changes, we disconnect the VPN Connection. But the only message in the log states:

  > 111 13:58:38.601 10/03/02 Sev=Info/4 CM/0x6310001F
  > Adapter address changed. Terminate secure connections

  We should have better log messages to debug this problem. The old message was removed, and the following two new messages were added.

  When the connection is established, we display the log message:

  > Address watch added for 10.10.10.10. Current addresses are 10.10.10.10,10.10.10.12.

  From the above message we know that the address used to establish the connection was 10.10.10.10. We also know that the system has two IP Addresses - 10.10.10.10, and 10.10.10.12.

  If the address 10.10.10.10 changes, we will disconnect the connection, and log the following message:

CORREIOS
0213
3690

Adapter address changed from 10.10.10.10. Current addresses are 10.10.10.12, 10.10.10.13.

- CSCdz23365

  The installation instructions at the following URL are incorrect if you are installing the VPN Client in fallback mode:

  http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_administration_guide_chapter09186a00800bd991.html#xtocid10

  IF MSGINA.DLL is the only GINA installed, then a line in the vpnclient.ini that says:

  INCOMPATIBLEGINAS=MSGINA.DLL

  does not make the client install in fallback mode, even if the GINA is also specified in the registry as being the GINA that is installed.

- CSCdz26371

  In a setup where a VPN Client is behind a natted device and connects to a VPN 3000 Concentrator using NAT-T (NAT Traversal), the Concentrator may think its behind a natted device as well and send keepalive packets to the VPN Client on destination port UDP 4500.

  The NAT-T feature helps devices determine whether NAT exists between IKE peers as well as where the NAT is. This information is negotiated in NAT-T payload. A VPN Client behind a natted device might fool the Concentrator into thinking that it is also behind a nat device. This might cause the Concentrator to send keepalive packets, which might get dropped by the NAT device on the VPN Client side.

- CSCdz41646

  The connection dialog should show the certificate name during the connection establishment. This lets the user know which certificate is being used to establish the VPN Connection.

- CSCdz56951

  General Packet Radio Service (GPRS) dialup environments require multiple VPN Client attempts for the tunnel to establish. The reasoning behind this is that as soon as VPN client receives an IP address from the GPRS RAS, it immediately attempts the IKE phase of the tunnel. However, having received an IP address from the RAS doesn't necessarily mean the GPRS link is operational. Therefore the 1st tunnel establishment fails and requires usually a 2nd attempt to establish the tunnel.

14.585
03/2005 - CN
CORREIOS
0214
3690

4584
J

Resolution:

Our normal behavior is to dial the RAS connection and then go to the next phase, which is IKE negotiations. But to resolve this issue, we will dial the RAS connection and then wait few seconds (user configured) before starting the IKE negotiations.

The default behavior of the VPN Client remains unchanged. But if users want to wait after dialing the RAS connection, they can do that by modifying the vpnclient.ini file. This file is located in the installation directory (generally "C:\Program Files\Cisco Systems\VPN Client"). Users will have to add another parameter under main as follows:

```
[main]
DialupWait=x
```

where x is in seconds. The default value is 0 seconds. If we do wait, the following info message is logged to the log viewer:

"Waiting x seconds per user request"

This wait would happen if the VPN Client is used to dial the connection, or if the VPN GUI is used to configure a third-party dialer for dialing the connection.

- CSCdz61884

  When setting up an IPSec tunnel with the VPNClient using the CLI parameter "notrayicon", the tunnel established indicator in the Windows 2000 machine's registry is not cleared after the tunnel has been terminated or timed out.

- CSCdz62411

  The VPN Client does not show the session as disconnected after the session is terminated from the VPN 3000 Concentrator.

- CSCdz72657

  It takes too long to establish the tunnel from a windows machine. Users would see that VPN connection hang for couple of seconds at "Contacting the gateway at a.b.c.d".

  This would occur only if XAuth is used for authentication. The Log Viewer would show a long delay between the following 2 messages:

  209 16:15:21.370 01/30/03 Sev=Info/4CM/0x63100015

  Launch XAuth application

  210 16:16:23.683 01/30/03 Sev=Info/4CM/0x63100017

RQS nº 43 - CN
CPMI - CORREIOS
Fls_Nº 0215
3690
Doc.

14583

XAuth application returned

Remember that the difference between the two messages above also represents the time users take to enter the password in the XAuth dialog box.

This should happen only intermittently.

Caveats Resolved in Release 3.6.3

- CSCdy77156

  With the MSI installer, you need to use the VPNCLIENT_EN.EXE file to update the MSI version. Running this executable does not function properly if you need to use a MSI transform.

- CSCdy86051

  TunnelEstablished registry value is supposed to reflect the state of the tunnel.

  The following problem was seen on Win XP with VPN Client v3.5 and v3.6.1:

  When you close windows during a VPN connection, the VPN Client doesn't change the TunnelEstablished value in reg.base from 1 to 0 during the windows "shut down". And when you then restart Windows the reg.base still says TunnelEstablished value = 1 even though the VPN is not established.

Caveats Resolved in Release 3.6.2.B

- CSCdy39938

  Split-DNS servername is not released by VPN Client version 3.6 on Windows NT after disconnecting from VPN.

- CSCdy54329

  Installing the 3.6 VPN Client on a Windows XP system that has Service Pack 1 applied may result in a Hardware Installation warning that the Deterministic Network Enhancer Miniport drivers are not signed. The installation can proceed without complication by clicking "Continue Anyway" at all of the warnings. There will be multiple warnings, the number will vary depending on the system configuration.

78-15450-01
CPMI - CORREIOS
0216
Fls -Nº
3690

14.582

- CSCdy78142

  In the v3.x VPN Client, the VPN Client always fails reauthentication after "New PIN mode" when using SDI SoftID software. The problem occurs because the VPN Client always uses the current tokencode with the new PIN when it should be using the next tokencode with the new PIN.

- CSCdy81700

  Unable to pass external (non-tunneled) traffic other than ICMP with split tunneling enabled on Mac OSX 10.2.x while connected with the VPN Client. Ping, nslookup, and traceroute still work to external addresses.

  The issue will not manifest over wireless or PPP. It is an issue with the checksum negotiated with the hardware of the newer platform hardware. The problem will not be seen on older platforms such as original iMacs.

Caveats Resolved in Release 3.6.2.A

- CSCdy29594

  If you are using Windows NT4 and the VPN Client and you connect to your ISP with the Multiple Line feature in the Dial-Up entry, for example to get up a multilink for ISDN, only one line gets connected when initiated from the VPN Client. Dialing from the Dial-Up program in Windows NT works fine.

- CSCdy49082

  The latest Red Hat beta release (code-named "null") will be based on the gcc 3.2 compiler, and kernel modules compiled with gcc 2.9x will not work with the kernel in this new release. Since the vpnclient distribution does not include all of the source for the vpnclient kernel module and for existing releases the binary portion of the kernel module is compiled with gcc 2.95.3, existing releases will not work on a gcc 3.2 based system.

- CSCdy61356

  When we try to use the Start Before Logon feature with the VPN Client 3.6.1 after bringing up the VPN connection and logging onto the network, we see an error "PPPtool.exe has generated errors and will be closed by Windows."

- CSCdy67438

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0217
Doc 3690

In the InstallShield Script file, we were trying to register the gina before we copied the vpnclient.ini file to the installed directory. Moved the copying of the INI files from routine UpgradeProfiles to routine OnFirstUIAfter before we made the call to routine SetupRegistry. This allowed the Gina registration process to obtain the information from the vpnclient.ini file before it registers the gina.

- CSCdy74287

  The v3.6.1.Rel VPN Client installation application does not appear to use the IncompatibleGinas line from the VPNCLIENT.INI file and will replace an "incompatible" GINA with the VPN Client GINA, csgina.dll. This will only occur at install time if the .INI file contains the RunAtLogon=1 line.

- CSCdy76318

  A new installation of the Linux VPN Client v3.6.2 does not compile because of missing files. After the v3.6.1VPN Client release, changes to the installation caused a problem in the Linux VPN Client. This issue is not easily apparent when overwriting a previous version of the client.

Caveats Resolved in Release 3.6.2

- CSCdy48192

  IPSec over TCP (cTCP) does not work with Release 3.6 or 3.6.1 of the Cisco VPN Client when running on Mac OS X 10.2.

- CSCdy51818

  While attempting to use a VPN Client 3.6 on a Mac OS X 10.2 Jaguar platform, Split Tunneling does not work. This only happens on the Mac OS X 10.2 platform. Mac OS X 10.1 performs appropriately.

- CSCdy55145

  The VPN Client sometimes sees DPD replies from the VPN Concentrator coming from reversed Public IP address from what the VPN Concentrator has. Issue goes away on its own and doesn't seem to cause disconnects.

- CSCdy59183

  The VPN Client with MacOS X 10.2 may fail to connect with the following error message, even when the kernel module is known to be loaded (verified with the "sudo kextstat" command):

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0218
Doc. 3690

"Could not attach to driver. Is kernel module loaded?"

This occurs on VPN Client 3.6.1 on MacOS X 10.2 with IPv6 enabled, and multiple network interfaces enabled.

Caveats Resolved in Release 3.6.1

This section lists the caveats fixed since Release 3.6. If you have an account on CCO you can check the status of any caveat by using Bug Navigator II.

To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Note Release 3.6.1 addresses multiple vulnerabilities for the VPN 3000 Series Concentrators and VPN 3002 Hardware Client. Please refer to the following URL for the details on the vulnerabilities addressed.
http://www.cisco.com/warp/public/707/vpnclient-multiple2-vuln-pub.shtml

- CSCdy14510

  On Windows 2000 machines with SMS 2.0 client installed and the Cisco VPN Client 3.5.2A set for Start Before Logon, when VPN Client tries to initiate the connection, the VPN Client hangs at "Initializing connection to your ISP".

- CSCdy28446

  When installing the VPN Client using a silent MSI install, the VPN Client does not detect if there is no TCP/IP stack installed. The VPN Client requires TCP/IP and will not function without it. If you do perform a silent install on a PC with no TCP/IP stack, after the install completes and reboots, you see the following error when you attempt to run the VPN Client:

  Cisco Systems VPN Client

  Windows Sockets initialization failed.

- CSCdy36987

47
CPMI - CORREIOS
Fls Nº 0219
3690

14.579

When a VPN tunnel is established, the Release 3.6 VPN Client may incorrectly send DNS queries to your ISP's DNS server instead of to your private DNS server. This results in failed attempts to connect to FTP, Telnet, or other servers when attempting connections by DNS name. Connecting by IP Address works fine.

This has been seen only with Windows XP and Dial-Up networking connections.

- CSCdy41127

  The VPN Client V3.6 does not work on interface en1 (Apple AirPort WiFi) card when running Macintosh OS X 10.2

Caveats Resolved in Release 3.6

This section lists the caveats fixed since Release 3.5.2.

- CSCdt00735

  Certificate Manager: Entrust VPN Connector displays an MD5 and SHA1 Fingerprint verification for a File-based certificate request from VPN Client. The VPN Client currently does not display this Fingerprint in the request.

- CSCdu20804

  One of the following error messages might occur when using the Release 3.5.1, 3.1, or 3.0 VPN Client on Windows NT or Windows 2000 with the Start Before Logon feature. After you establish the Client connection and then attempt to logon to the network, you might see one of the following errors messages:

  - "A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available." This means that you are logged in at the desktop, and you can see network drives and browse the network.
  - "The system cannot log you on now because the domain YOURDOMAIN is not available." This happens less often, but you can't log in at all.

  At present, the only way to prevent these errors is to establish the VPN connection, then wait up to 1 minute before attempting the network logon.

n° 03/2005 - CN
CPMI - CORREIOS
Fls 0220
3690

14.578
1

- CSCdu36579

  When Outlook Express is set to Work Offline mode and you attempt to synchronize any folder with your home Exchange server, synchronization fails on any folder that has changes. It is successful on any folder that is already synchronized.Outlook reports a generic Network Error for each folder that fails.

  Cisco VPN Client NATs the IP Address of the host machine it is installed on. But the communication between MS Exchange to MS Outlook is not NAT-compatible. However, any communication initiated by Outlook (for Exchange) has no problem. Only the connections initiated by Exchange (for Outlook) have problems. Any time a new mail arrives on Exchange server, it sends a notification to Outlook. Since this communication is not NAT-compatible, it is dropped. As a result of this, the Outlook client is not notified of any new mail until it contacts the Exchange server. Outlook contacts the Exchange server anytime the user makes any modifications, such as switching folders, sending mail, clicking the "Send/Receive" button etc

  To overcome this problem, Microsoft advises disabling Exchange-to-Outlook notifications by updating MAPI property called PR_DISABLE_WINSOCK. This forces Outlook to poll the Exchange server every 60 seconds.

  Microsoft identified a problem in MS Outlook 2000 as the cause of this issue. If Outlook is polling and synchronizing at the same time, Outlook hangs. Microsoft said that this problem is fixed in Outlook 2002. Since the fix for this problem was very complicated, Microsoft is not planning on back-porting the fix to Outlook 2000.

  To remedy this problem, we provide the users with an option to enable or disable Outlook to Exchange polling. The default behavior is to enable Outlook to Exchange polling. If you prefer synchronization over "new mail notifications", you can override the default behavior by adding the following variable in vpnclient.ini file (present in the client installation directory):

  [main]
  OutlookNotify=1

  The IPSec Dialer (or CLI) defaults to polling if this variable is not present or if its value is 0.

005 - CN
CORREIOS
0221
3690

- CSCdu57246

  A mechanism is needed to allow removal of a pre-defined IncompatibleGina.

  Currently, no method exists to remove a GINA from the predefined IncompatibleGinas list that ships with a VPN Client, even though the vendor has fixed the GINA and the customer now wants to use it in non-FallBack mode with the Client. No workaround currently exists.

- CSCdu61922

  If ZoneAlarm is uninstalled on a Windows 98, Windows ME, Windows NT 4 or Windows 2000 PC, then reinstalled, after rebooting the PC and launching the VPN Client, the following message might appear:

  "The VPN subsystem is not available. A connection to the concentrator will not be possible."

  Click OK, then click Connect on the VPN Client; the connection continues normally.

- CSCdu80463

  Transferring large files fails when using a VPN Client connection over a DSL/PPPoE connection. For example, if you use FTP to try to PUT a large file, it stalls and never completes. FTP GETs seem to be OK.

  This problem has been seen on Win 2000 using the Verizon DSL software (WinPoET) and Windows XP RC1 using the native PPPoE adapter. There have also been reports that this problem also occurs with NTS EnterNet PPPoE software.

  Workaround:

  For WindRiver WinPoET and NTS EnterNet, the following workaround is available.

  - *For systems other than Windows XP*, modify the MTU on the PPPoE adapter by explicitly changing or creating the following registry key:

    ```
    HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber>
    adapter(000x):
            Value: MaxFrameSize
            Value type: DWORD
            Data: 1400 (or less - you may need to experiment)
    ```

  - *For Windows XP*, the SetMTU utility does this function automatically.

0222
3690

14.576

Caution Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable.

- CSCdv11350

  If you install a new Network Interface Card (NIC) on Windows 2000 or XP after the VPN Client is installed, the VPN Client starts to connect and complete user authentication, but it then appears stuck at "Securing Communications Channel...". When this happens, these events appear in the Event Log:

  35 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xE300006D
  Cannot match Policy Entry:
  local host=IP ADDR=0.0.0.0, lcl_port = 0
  remote host=IP ADDR=0.0.0.0, dst_port = 0

  36 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xA3000001
  Failed to initiate negotiation.

  37 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xE3000002
  Function initialize_qm failed with an error code of 0x00000000 (INITIATE:825)

- CSCdv63980

The VPN Client cannot use backup servers during connection attempts if it is configured to use IPSec over TCP for NAT Transparency (TunnelingMode=1).

- CSCdv75911

  If the VPN Client is configured to use IPSec over TCP for NAT Transparency, (Tunneling Mode=1), you cannot establish a connection using PPP or Ethernet if you use a large certificate (such as one created by a Microsoft CA).

- CSCdv76902

  If a session is already active when the Cisco Integrated Client firewall is enabled (either on the VPN Client or by policy pushed down from the Concentrator (CPP), that session is permitted to continue sending outbound packets, as long as they are not blocked by an outbound rule.

  However, if the first packet sent after the firewall is enabled is inbound, the firewall does not allow the packet.

ROS nº 03/2003 - 0223
CPMI - CORREIOS
Fls Nº
3690

- CSCdv77711

  On a Windows 95 PC the following error may occur during a connection:

  CVPND caused an invalid page fault in module <unknown> at 0000:0400225b

  If this message appears, reboot the computer. The VPN Client then connects to the Concentrator with no problem.

- CSCdv81538

  If BlackICE Defender version 2.9 is on Windows XP and the VPN Client is reinstalled, the computer may display a blue screen (failure) upon reboot.

- CSCdv86123

  If you are using the enroll command for certificates and you enter information in all fields, you might get a segmentation fault.

- CSCdx31313

  The following error may occur on a Windows 95 PC when connected to the Concentrator:

  CVPND caused an invalid page fault in module <unknown> at 0000:100022e5.

  Registers:

  EAX=00000102 CS=0137 EIP=100022e5 EFLGS=00010206

  EBX=00000001 SS=013F ESP=011ED258 EBP=011EFF94

  ECX=CB6F9ACC DS=013F ESI=00000000 FS=2757

  EDX=CB6F9ACC ES=013F EDI=100022B6 GS-0000

  Bytes at CS:EIP

- CSCdx39302

  The Microsoft error messages that appear when you attempt to install the VPN Client using the Windows Installer do not indicate that Windows 95, Windows 98, Windows Me, and Windows NT (SP3) are not supported for Release 3.6 of the VPN 3000 Series Concentrator.

  These errors occur on PCs that do *not* have the Microsoft Windows Installer installed (Windows 95, Windows 98 and Windows NT (SP3)) or that have an older version of MSI installed (Windows Me). Once the errors occur and you click OK, no other messages are displayed and the installation is aborted.

CPMI - CORREIOS
Fls. 0224
3690

This is a Microsoft issue. The messages are as follows:

- On Windows 95 and Windows 98, when you attempt to run vpnclient_en.exe you see the following message:

  "Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."

- On Windows NT SP3, when you attempt to run vpnclient_en.exe you see the following message:

  "Cannot find the file instmsiw.exe (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."

  followed by:

  "Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."

- On Windows Me, when you attempt to run vpnclient_en.exe you see:

  "This installation package cannot be installed by the Windows Installer service.You must install a Windows service pack that contains the newer version of the installer service"

- CSCdx50376

  The following error message occurs if the MSI installation is canceled after DNE is installed but before the installation has completed:

  "Error in Custom Action. The library CSGina.dll is invalid or could not be found."

  When this message appears, click OK; the rollback continues with no further errors.

- CSCdx58271

  After installing the VPN Client using the MSI installer, rebooting, then launching the installer again, a box appears offering to Repair or Remove. If Repair is selected, the installer attempts to reinstall the Client. During the "Repair", the following message box appears:

ECT/ECT nº 03/2005 - CN
CPMI - CORREIOS
0225
Fls. Nº
3690

14.573

Deterministic Network Enhancer

Add plug-in failed

Click the OK button and another message appears:

Error 1722. There is a problem with this Windows Installer Package...

Click the OK button and the installer rolls back without another message.

NetworkICE and DNE are researching this issue.

- CSCdx60297

  Using Auto-initiate to connect the client before logging into a domain on Windows 95 may result in no VPN Client tray icon appearing (yellow padlock). The client is connected and can be launched from the start menu to view status or disconnect

- CSCdx66747

  If the VPN Client is uninstalled, the Computer must be rebooted before attempting to reinstall the Client. If the Computer is not rebooted between uninstalling and reinstalling the Client, the Client will not be able to connect to the Concentrator.

  If this situation occurs, uninstall the Client, reboot the PC, then reinstall the Client and reboot after the reinstall.

- CSCdx83871

  Using a LAN-to-LAN configuration with Digital Certificates, sending entire chain does not work. If set to send Ident only, it works fine.

- CSCdx86987

  When using the VPN Client Certificate Manager to perform an SCEP enrollment to a CA that was previously enrolled to, the CA's URL appears incomplete as "http:/".

- CSCdx87075

  The 3.6 VPN Client cannot connect with digital certificates if it is sending the certificate chain.

  Workaround

  Disable "Send CA certificate chain" on the client and manually install the certificates needed on the Concentrator to validate the client's ID certificate.

  To disable Send CA certificate chain on the client, do the following:

78-15450-01 CN
CPMI - CORREIOS
Fls. Nº 0226
3690

Step 1 Click Options->Properties

Step 2 Change to the Authentication Tab and uncheck the option near the bottom of the dialog.

- CSCdx89079

  If ZoneAlarm version 2.6.362 is installed on the PC the following Blue Screen might occur:

  Stop: 0000001e (80000003, 80452e64, 00000000, 00000000)

  kmode_exception_not_handled

  ***Address 80452e64 base at 80400000, datestamp 384d9b17 -- ntoskrnl.exe

- CSCdx89903

  The VPN Client (using the Windows Installer - MSI) requires that Windows NT 4.0 users *must* use Service Pack 6 (SP6). The message that appears when installing on NT 4.0 SP3 - SP5 does *not* say that SP6 is required.

- CSCdx89962

  Problems have occurred on some Windows NT systems when using AES encryption. The PC may blue screen after sending data using AES. The problem is under investigation.

  Workaround:

  Add the following line into the vpnclient.ini file in the [Main] section and restart the computer:

  ExcludeAESProps=1

  The vpnclient.ini file is in the following directory:

  c:\Program Files\Cisco Systems\Vpn Client

  This line keeps the VPN Client from sending any AES proposals to the Secure Gateway that keep AES from being negotiated. Keep in mind that the Secure Gateway must be configured for a different encryption protocol.

- CSCdx92053

  The Windows Installer (MSI) version of the v3.6 VPN Client install does not register IPSECDIALER.EXE in the following registry key as previous versions of the VPN Client did:

CPM 55 CORREIOS
Fls. Nº 0227
3690

14.571

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ipsecdialer.exe

This occurs *only* when using the Windows Installer (MSI). The InstallShield version does not exhibit this problem.

- CSCdy08772

  The VPN Client is adding bogus information into the Backup Server list when the VPN 3000 Concentrator sends a list of backup servers and is configured to use the list. If you look in the .PCF file after a connection, you will see something similar to this:

  BackupServer=200.70.50.199,200.70.50.200,200.70.50.250,Version,3.6.int_76,built,by,yurname,on,Jul,02,2002,19:00:2400.compp

Documentation Updates

The following VPN Client documentation has been updated for Release 3.6. These documents contain information for all platforms on which the VPN Client runs:

- *VPN Client Administrator Guide, Release 3.6*
- *VPN Client User Guide for Windows, Release 3.6*

The most recent information specifically for the VPN Client for Linux, Solaris, and Mac OS X is in the following document, which was not updated for Release 3.6:

- *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*

Related Documentation

- *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 3.6*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management, Release 3.6*
- *VPN 3000 Series Concentrator Getting Started, Release 3.6*

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-15450-01
Fls. Nº 0228
3690
Doc.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

14.520
57
CPML - CORREIOS
Fls. Nº 0229
3690

14.569

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online

ROS nº 03/2005 - CN
CPMI 78-15450-01 CORREIOS
0230
Fls. Nº
3690
Doc.

14.568

technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

59
CPMI - CORREIOS
0231
Fls. Nº
3690

14.567

http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Copyright and Trademark Information

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

CPMI - CORREIOS
Fls. Nº 0232
3690

14.566
1

Switch Tipo 5 doc 11

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0233
Doc. 3690

Cisco Systems

14.565

Data Sheet

CiscoWorks **VPN Monitor** 1.2

Enterprises have recognized the dramatic benefits of virtual private networks (VPNs) using IP Security (IPSec) to reduce costs and secure their networks. Now, as IPSec VPNs become business critical, enterprises need strong management tools to monitor the health of IPSec tunnels and central-site VPN devices.

Introduction

Once a VPN has been deployed, network administrators must be able to monitor the health of the tunnels and VPN devices to ensure optimal VPN services. They need the following information:

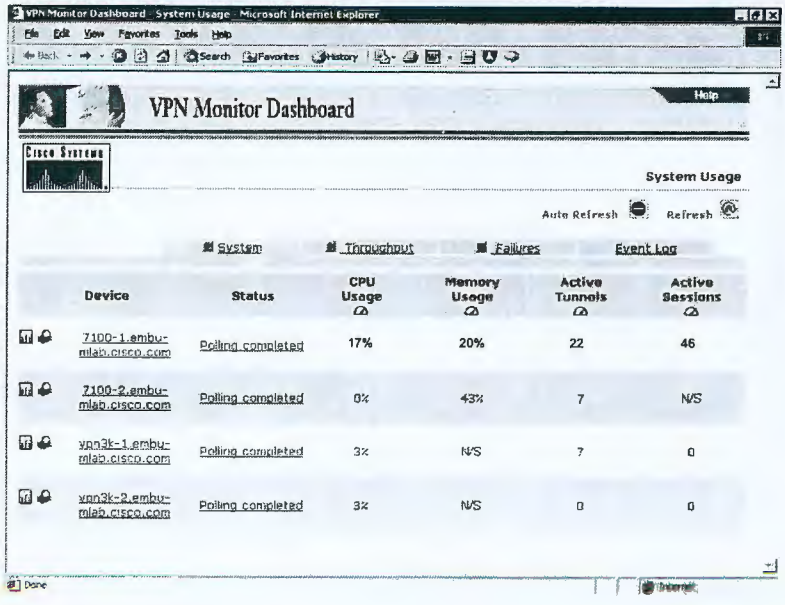
- Number of operational tunnels
- Throughput of individual tunnels
- Status of security negotiations and sessions
- VPN device performance status
- Performance threshold violations

Network managers can generate special reports on VPN-related problems to provide visibility on Internet Key Exchange (IKE), encryption, encapsulation, and certificate problems. Network managers need ongoing reports on current VPN activity, outages, VPN failures, signs of impending failures, and activity history.

CiscoWorks VPN Monitor is a Web-based management tool that allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. CiscoWorks VPN Monitor manages VPNs that are configured on Cisco VPN 3000 concentrators, and Cisco 1700, 2600, 3600, 7100, 7200, or 7400 Series routers. Multiple devices can be viewed from an easy-to-use dashboard configured on a Web browser. After the dashboard is configured, CiscoWorks VPN Monitor continuously collects data from the devices it manages over a rolling seven-day window. Operational status, performance, and security information can be viewed at a glance, providing status information on IPSec VPN implementations.

The dashboard allows network administrators to drill down to further analyze each device's performance and its current IPSec connections. Administrators

Figure 1
CiscoWorks VPN Monitor Dashboard



ROS nº 03/2005 - CN
CPMI - CORREIOS
0234
Fls: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.564

can use this drill-down capability to view device CPU and memory performance, tunnel throughput, failure events, threshold violations, and active tunnels on a device. Data collected from VPN devices can also be viewed in detailed graphs that display important parameters related to VPN operation.

CiscoWorks VPN Monitor supports the commonly deployed VPN tunneling protocols, including the IETF Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and IPSec.

Features and Benefits

Flexible Monitoring

CiscoWorks VPN Monitor's configuration flexibility allows network administrators to set polling and graphing intervals to best reflect the network performance of the network and the graphical user interface of CiscoWorks VPN Monitor. The types of monitoring range from the percent utilization of a CPU, to the throughput of a VPN concentrator or router, to the number of users with established connections. Other variables that can be tracked include:

- System resources—average and maximum memory available and CPU utilization percentage per device
- Traffic throughput—average and maximum of encrypted traffic
- Statistics—number of sites that are online, number of sessions established, number of IKE and session failures, and number of current security errors

The dashboard can also provide troubleshooting information. Auto-refreshing Web-based status reports provide detailed information on conditions such as the number of session failures or IKE failures by peer. You can set warnings and alerts based on user-defined threshold values.

Multidevice Comparison

CiscoWorks VPN Monitor provides a convenient way to view important statistics of multiple VPN termination devices in a single dashboard. This capability enables administrators to quickly correct for devices with the highest CPU or memory usage. The multidevice view gives the administrator an aggregated summary of active VPN tunnels and sessions.

Supported Cisco Devices

- Cisco VPN 3000 concentrators with the 2.5.2f software image or later
- Cisco 7100, 7200, or 7400 Series routers with Cisco IOS® Software Release 12.1.(5a)E or later
- Cisco 1700, 2600, and 3600 Series routers with Cisco IOS Software Release 12.2(4)T or later

System Requirements

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

Ordering Information

CiscoWorks VPN Monitor is available exclusively as part of the CiscoWorks VPN/Security Management Solution (VMS).

Detailed ordering information is available in the VMS product bulletin at http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0235
Fls Nº
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.563
J

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

0236
3690

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

14.562
1

Roteador Tipo 1 doc1

FLS. Nº 0237
3690

Cisco Systems

14.561

Data Sheet

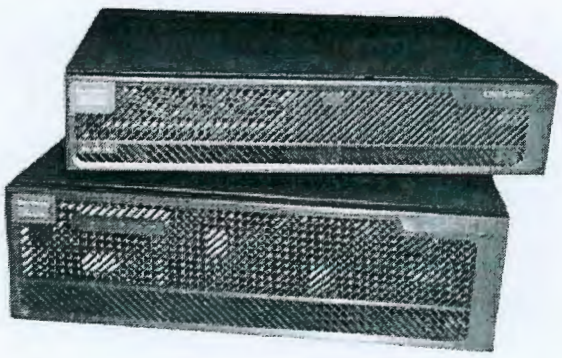
Cisco 3700 Series **Multiservice** Access Routers

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 that enable flexible and scalable deployment of new e-business applications for the Full Service branch office. The Cisco 3700 Series routers optimize the branch office with high performance routing, integrated low density switching, Security, Voice, IP telephony, Video and Content Networking in a single integrated solution. This unique integrated design enables enterprise customers to incrementally adapt to evolving business needs by enabling important services delivered by Cisco IOS®, such as Quality of Service (QoS), IP Multicast, VPN, Firewall, and Intrusion Detection, with the performance required for tomorrows business challenges. The Cisco 3700 Multiservice Access Routers are based on the same modular concepts as the Cisco 3600 Series but enable dramatically higher levels of performance and service integration for 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-density service modules (HDSM), and support for multiple Advanced Integration modules (AIMs) to deliver the highest levels of service density for the enterprise branch office today. Improving on the success of the Cisco 3600 Series' modular architecture, these highly integrated platforms deliver a compelling value proposition with by integrating components previously purchased separately, such as two fixed 10/100 LAN ports and additional memory. With the options of 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 3700 offers many flexible options to enable high densities of services. Providing support for the majority of LAN and WAN interfaces available today on the Cisco 3600 Series platforms reinforces Cisco investment protection promise and maximizes the flexibility of these platforms for the future.

0238
Els. N° 3690

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.560
J

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)

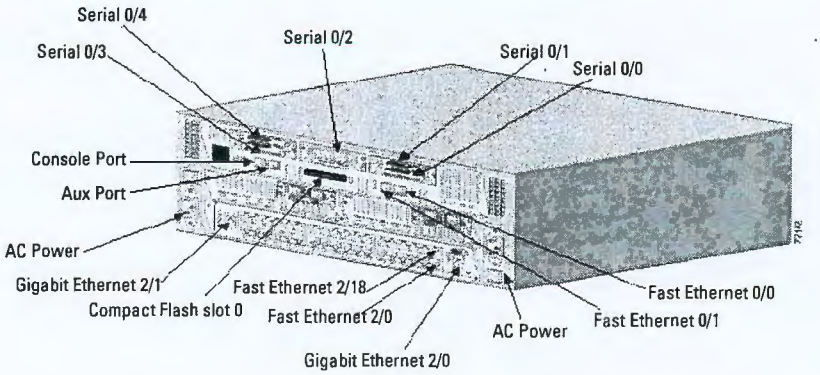
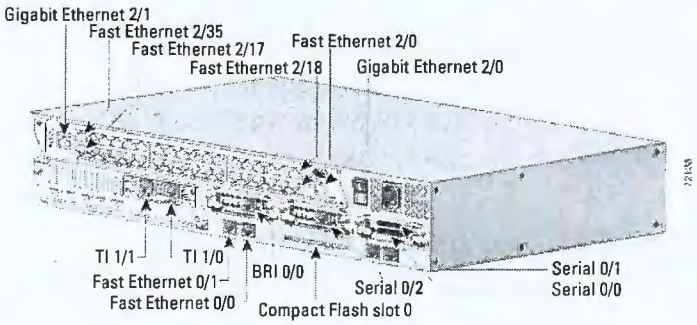


Figure 3 Cisco 3725 Multiservice Access Router (shown with optional interfaces)



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.

CPMI - CORREIOS
Fls. Nº 0239
3690
Doc.

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0240
Doc. 3690

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

POST & DRAM - CN
CPU - ORDER NO.
PS. NO. 0211
3690 -
Doc.

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.558
J

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.

CPMI - CORREIOS
Fls. Nº 0242
3690
Doc.

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

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 solutions supports the features essential to VPNs—IPSec data encryption, tunneling, broad certificate authority support for

0243
3690

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

84.556

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.

CPMI - CORREIOS
0244
Fls. Nº
3690

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.555

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

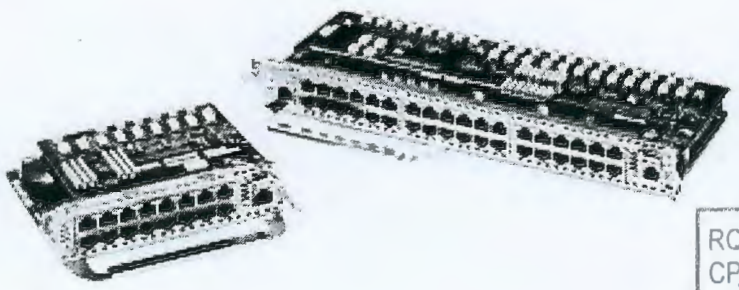
The Cisco 3700 Series offers an optional 16-port 10/100 EtherSwitch network module (NM), or an optional 36-port 10/100 EtherSwitch high density service module (HDSM), both of which leverage the proven Cisco Catalyst technology. The EtherSwitch NM/HDSM hardware supports 802.1p Layer 2 prioritization, 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



ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0245
3690
Doc.

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

044.554

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.

Rubrica nº 03/2006 - CN
CPMI - CORREIOS
0246
Fls. Nº
3690
Doc.

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.553

Figure 5 Cisco 3700 Full Serivce Branch integrated capabilities

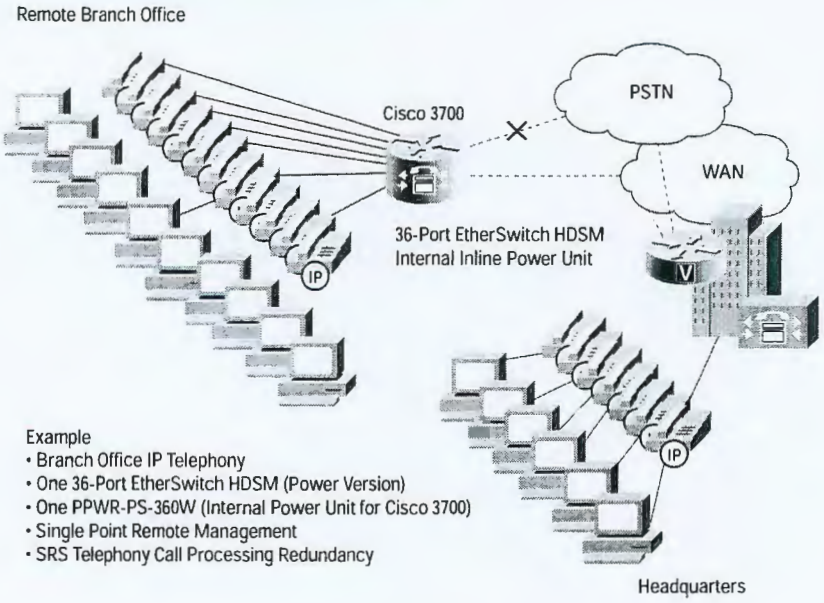
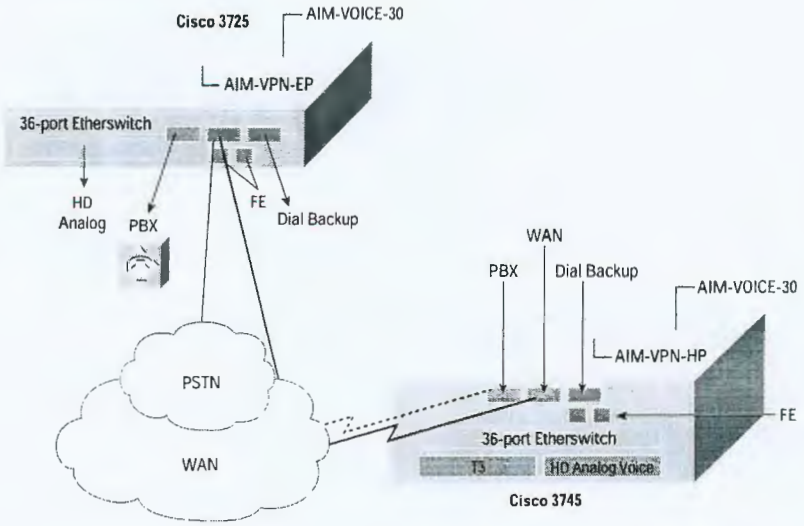


Figure 6 Full Service Branch scenarios



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0247
3690

Cisco Systems, Inc.
All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.552

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

ROS nº 03/2003 - CN
CEMI - CORREIOS
Fls. Nº 0248
3690
Doc.

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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)

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0249
3690
Doc.

14.550

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

nº 03/2005 - CN
CPMI - CORREIOS
Fls 0250
3690

Cisco Systems, Inc.
All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.549

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

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls Nº 0251
3690
DOC

All contents are Copyright © 2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14,548

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliate in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

CONFIDENTIAL - CN
FEB 2008
025
3690

04.03 BW9112

44.547

Roteador Tipo 1 doc 2

CORREIOS
Fls. Nº 0253
3690

Cisco Systems, Inc.(R) Close Window

Feedback | Help

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:

Major Release	12.3
Release	12.3(1)
Platform	3745
Feature Set	ENTERPRISE PLUS IPSEC 3DES

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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
0254
Fls Nº
3690
Doc.

14.545

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
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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0255
3690

14.544

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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0256
Doc. 3690

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

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0257
Doc. 3690

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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0258
Doc. 3690

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0259
3690

14.540

- 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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 360
DOC 3690

14.539

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

ROS nº 03/2005 - CN
CPMI - CORREIOS
0261
Fls Nº
3690

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
0262
Fls. Nº
3690

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

14.537

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0263
3690

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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3690
Doc

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

nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0265
3690

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0266
3690
Doc.

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

14.533

nº 03/2005 - CN
CPMI CORREIOS
0267
Fls Nº
3690
Doc.

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0268
3690
Doc.

SIP: ISDN Suspend/Resume Support
Snapshot routing
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
SNMP Version 3
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+

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0269
Doc. 3690

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

14.530

MESS nº 03/2005 - CN
CPMI CORREIOS
0270
Fls Nº
3690

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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0271
3690

Close Window

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0272
3690
Doc.

14.527
J

Roteador Tipo 1 doc 3

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 0273
3690
Doc.

Cisco Systems, Inc.(R) Close Window

Feedback | Help

MIB Locator

Make Selections to get to a Specific Cisco IOS Release:

Release: 12.3(1a)

Platform Family: 3745

Feature Set: ENTERPRISE PLUS IPSEC 3DES

New Search

Download all V1 , V2 MIBs

mage Information

c3745-jk9s-mz.12.3-1a

Get list of features for this image from Cisco Feature Navigator

MIBS Supported in this Image	Details	Download MIB	
ATM-MIB		V1	V2
BGP4-MIB		V1	V2
BRIDGE-MIB		V1	
CISCO-AAA-SESSION-MIB		V1	V2
CISCO-AAL5-MIB		V1	V2
CISCO-ACCESS-ENVMON-MIB		V1	V2
CISCO-ALPS-MIB		V1	V2
CISCO-ASPP-MIB	Note		
CISCO-ATM-EXT-MIB		V1	V2
CISCO-ATM-PVCTRAP-EXTN-MIB		V1	V2
CISCO-BGP4-MIB		V1	V2
CISCO-BSC-MIB		V1	V2
CISCO-BSTUN-MIB		V1	V2
CISCO-BULK-FILE-MIB		V1	V2
CISCO-BUS-MIB		V1	V2
CISCO-CALL-APPLICATION-MIB		V1	V2
CISCO-CALL-HISTORY-MIB		V1	V2
CISCO-CAR-MIB		V1	V2
CISCO-CAS-IF-MIB		V1	V2
CISCO-CDP-MIB		V1	V2
CISCO-CIRCUIT-INTERFACE-MIB		V1	V2
CISCO-CLASS-BASED-QOS-MIB		V1	V2
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB		V1	V2
CISCO-CONFIG-COPY-MIB		V1	V2
CISCO-CONFIG-MAN-MIB		V1	V2
CISCO-DIAL-CONTROL-MIB		V1	V2
CISCO-DLCSW-MIB		V1	V2
CISCO-DLSW-EXT-MIB		V1	V2

ROS nº 03/2005 - CN
CPMI - CORREIOS
0274
Fls Nº
Doc. 3690

CISCO-DLSW-MIB		V1	V2
CISCO-DSP-MGMT-MIB		V1	V2
CISCO-DSPU-MIB		V1	V2
CISCO-ENTITY-ASSET-MIB		V1	V2
CISCO-ENTITY-EXT-MIB		V1	V2
CISCO-ENTITY-VENDORTYPE-OID-MIB		V1	V2
CISCO-ENVMON-MIB		V1	V2
CISCO-FLASH-MIB		V1	V2
CISCO-FRAME-RELAY-MIB		V1	V2
CISCO-FRAS-HOST-MIB	Note		
CISCO-FTP-CLIENT-MIB		V1	V2
CISCO-H323-TC-MIB		V1	V2
CISCO-HSRP-EXT-MIB		V1	V2
CISCO-HSRP-MIB		V1	V2
CISCO-ICSUDSU-MIB		V1	V2
CISCO-IETF-ATM2-PVCTRAP-MIB		V1	V2
CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	Note		
CISCO-IETF-IP-FORWARD-MIB		V1	V2
CISCO-IETF-IP-MIB		V1	V2
CISCO-IETF-NAT-MIB		V1	V2
CISCO-IMAGE-MIB		V1	V2
CISCO-IP-STAT-MIB		V1	V2
CISCO-IPMROUTE-MIB		V1	V2
CISCO-IPSEC-FLOW-MONITOR-MIB		V1	V2
CISCO-IPSEC-MIB		V1	V2
CISCO-IPSEC-POLICY-MAP-MIB		V1	V2
CISCO-ISDN-MIB		V1	V2
CISCO-ISDNU-IF-MIB		V1	V2
CISCO-LEC-DATA-VCC-MIB		V1	V2
CISCO-LEC-EXT-MIB		V1	V2
CISCO-LECS-MIB		V1	V2
CISCO-LES-MIB		V1	V2
CISCO-MEMORY-POOL-MIB		V1	V2
CISCO-MOBILE-IP-MIB		V1	V2
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	Note		
CISCO-NTP-MIB		V1	V2
CISCO-PIM-MIB		V1	V2
CISCO-PING-MIB		V1	V2
CISCO-POP-MGMT-MIB		V1	V2
CISCO-PPPOE-MIB		V1	V2
CISCO-PROCESS-MIB		V1	V2
CISCO-PRODUCTS-MIB		V1	V2
CISCO-QLLC01-MIB		V1	V2
CISCO-QUEUE-MIB		V1	V2
CISCO-RAS-MIB	Note		
CISCO-RSRB-MIB		V1	V2
CISCO-RTTMON-MIB		V1	V2
CISCO-SAA-APM-MIB		V1	V2

$4.5.25

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0275
3690
Doc.

CISCO-SDLLC-MIB		V1	V2
CISCO-SIP-UA-MIB		V1	V2
CISCO-SMI		V1	V2
CISCO-SNADLC-CONV01-MIB	Note		
CISCO-SNAPSHOT-MIB		V1	V2
CISCO-STACKMAKER-MIB		V1	V2
CISCO-STUN-MIB		V1	V2
CISCO-SYSLOG-MIB		V1	V2
CISCO-TC		V1	V2
CISCO-TCP-MIB		V1	V2
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB		V1	V2
CISCO-VLAN-MEMBERSHIP-MIB		V1	V2
CISCO-VOICE-ANALOG-IF-MIB		V1	V2
CISCO-VOICE-ATM-DIAL-CONTROL-MIB		V1	V2
CISCO-VOICE-COMMON-DIAL-CONTROL-MIB		V1	V2
CISCO-VOICE-DIAL-CONTROL-MIB		V1	V2
CISCO-VOICE-DNIS-MIB	Note		
CISCO-VOICE-ENABLED-LINK-MIB		V1	V2
CISCO-VOICE-FR-DIAL-CONTROL-MIB		V1	V2
CISCO-VOICE-IF-MIB		V1	V2
CISCO-VOICE-NUMBER-EXPANSION-MIB	Note		
CISCO-VPDN-MGMT-EXT-MIB		V1	V2
CISCO-VPDN-MGMT-MIB		V1	V2
CISCO-VSIMASTER-MIB		V1	V2
CISCO-VTP-MIB		V1	V2
DIAL-CONTROL-MIB		V1	V2
DLSW-MIB		V1	V2
ENTITY-MIB		V1	V2
ETHERLIKE-MIB		V1	V2
EVENT-MIB		V1	V2
EXPRESSION-MIB		V1	V2
FUNI-MIB	Note		
IC-RMON-MIB			V2
IF-MIB		V1	V2
IGMP-STD-MIB		V1	V2
IMA-MIB		V1	V2
INT-SERV-GUARANTEED-MIB		V1	V2
INT-SERV-MIB		V1	V2
IP-FORWARD-MIB		V1	V2
IPMROUTE-STD-MIB		V1	V2
ISDN-MIB		V1	V2
LAN-EMULATION-CLIENT-MIB		V1	V2
MIP-MIB	Note		
MPLS-LDP-MIB		V1	V2
MPLS-LSR-MIB		V1	V2
MPLS-TE-MIB		V1	V2
MPLS-VPN-MIB		V1	V2
MSDP-MIB		V1	V2

14.524

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0276
3690

NOTIFICATION-LOG-MIB		V1	V2
NOVELL-IPX-MIB		V1	
NOVELL-RIPSAP-MIB		V1	
OLD-CISCO-APPLETALK-MIB		V1	
OLD-CISCO-CHASSIS-MIB		V1	
OLD-CISCO-CPU-MIB		V1	
OLD-CISCO-DECNET-MIB		V1	
OLD-CISCO-FLASH-MIB		V1	
OLD-CISCO-INTERFACES-MIB		V1	
OLD-CISCO-IP-MIB		V1	
OLD-CISCO-MEMORY-MIB		V1	
OLD-CISCO-NOVELL-MIB		V1	
OLD-CISCO-SYSTEM-MIB		V1	
OLD-CISCO-TCP-MIB		V1	
OLD-CISCO-TS-MIB		V1	
PIM-MIB		V1	V2
RFC1213-MIB		V1	
RFC1231-MIB		V1	
RFC1243-MIB		V1	
RFC1253-MIB		V1	
RFC1315-MIB		V1	
RFC1381-MIB		V1	
RFC1382-MIB		V1	
RFC1406-MIB		V1	
RFC1407-MIB		V1	V2
RFC1595-MIB		V1	V2
RMON-MIB		V1	V2
RMON2-MIB		V1	V2
RS-232-MIB		V1	V2
RSVP-MIB		V1	V2
SMON-MIB		V1	V2
SNA-SDLC-MIB		V1	V2
SNMP-FRAMEWORK-MIB		V1	V2
SNMP-NOTIFICATION-MIB		V1	V2
SNMP-PROXY-MIB	Note		
SNMP-TARGET-MIB		V1	V2
SNMP-USM-MIB		V1	V2
SNMP-VACM-MIB		V1	V2
SNMPv2-MIB		V1	V2
SOURCE-ROUTING-MIB		V1	V2
TCP-MIB		V1	V2
UDP-MIB		V1	V2
XGCP-MIB		V1	V2

14.523

Close Window

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 3277
Doc. 3690

14.522
J

Roteador Tipo 1 doc 4

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0278
Doc: 3690

Cisco Systems

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.

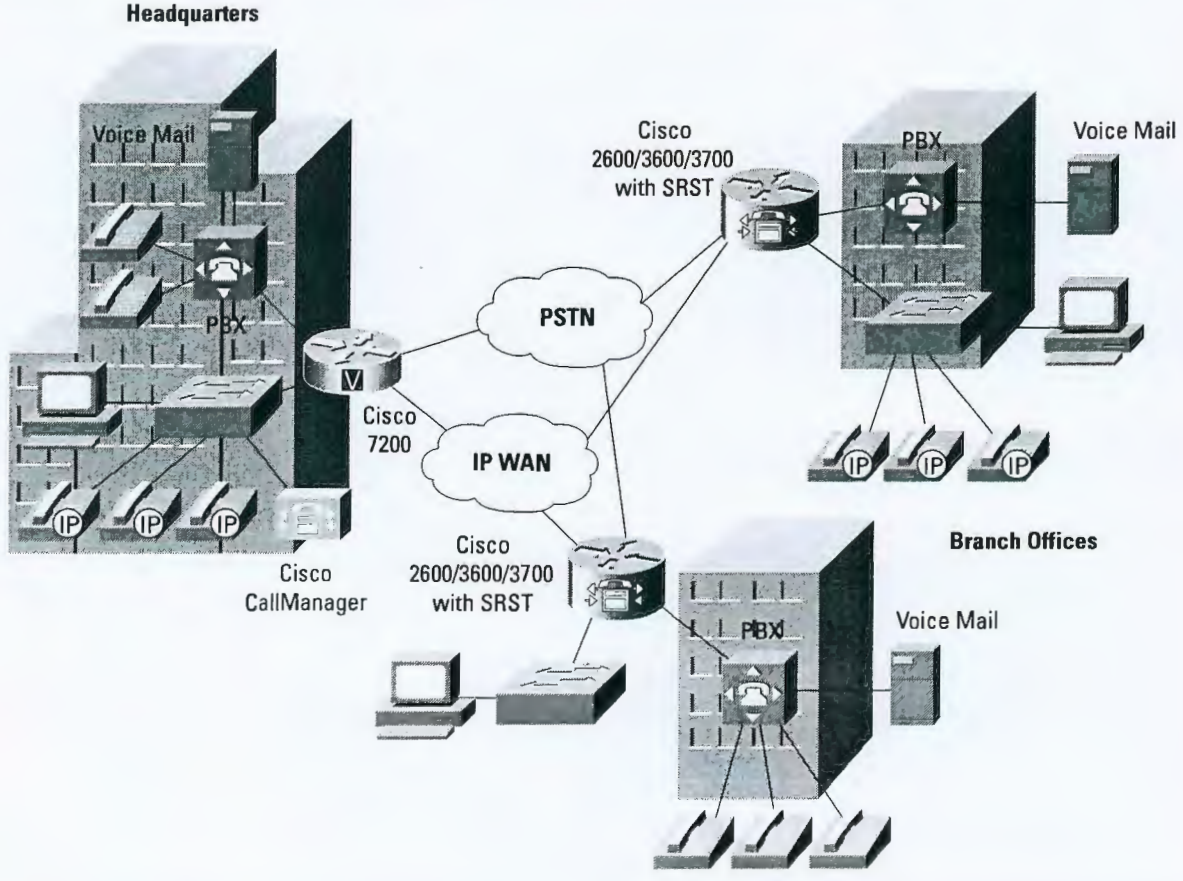
RQS nº 03/2005 - CN
CPMI - CORREIOS
0279
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

CPMI - CORREIOS
Fls. Nº 0280
3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.519

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

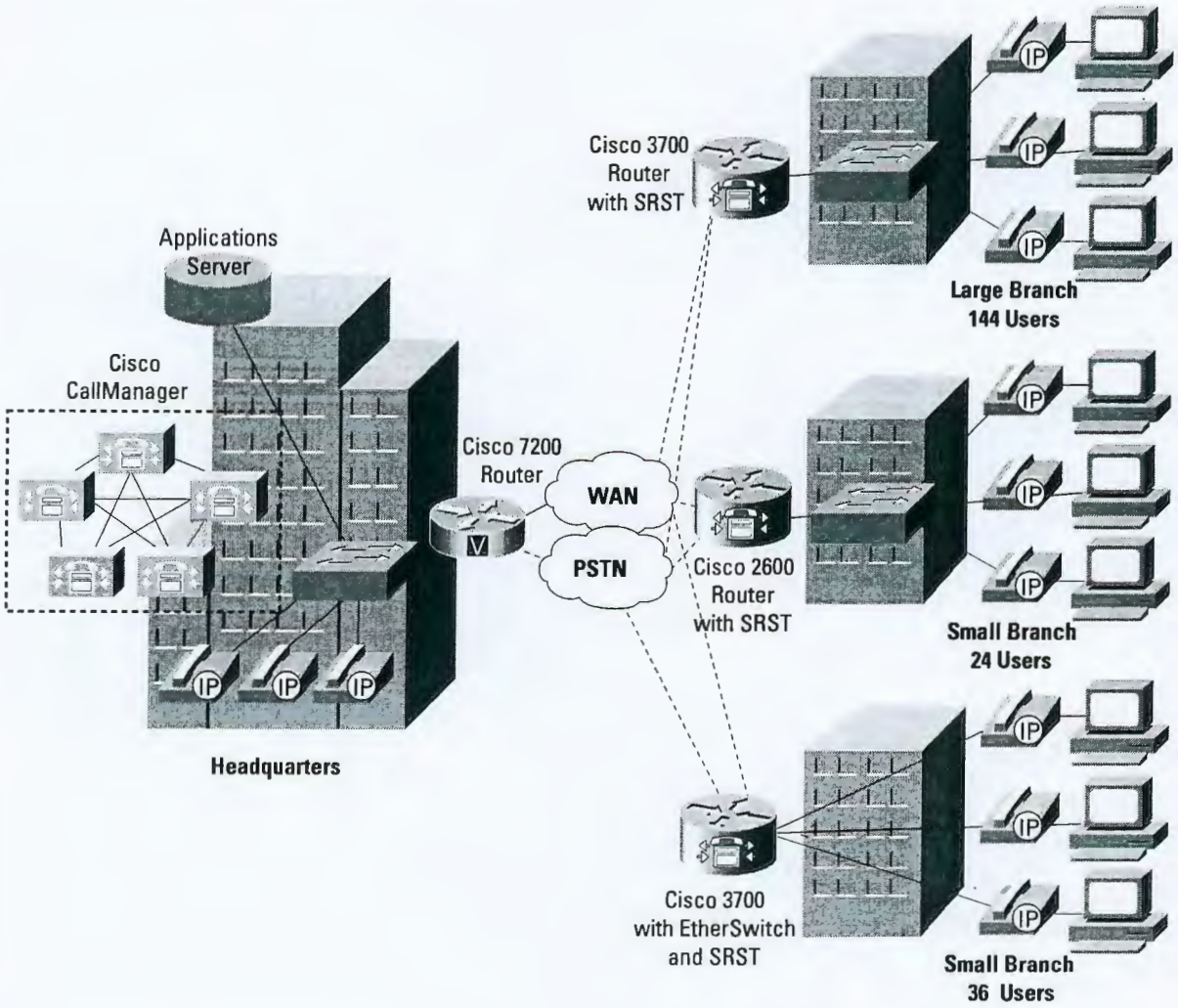
Survivable/Standby Remote Site Telephony (SRS Telephony)

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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0281
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

R S nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0282
3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.537

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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0283
FIS. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 MelCAS	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

ROS nº 03/2005 - CN
CPMI - CORREIOS
0284
FLS Nº 3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0285
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.534

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0286
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.513

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	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

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)

RQS nº 03/2005 - CN
CPMI - CORREIOS
0287
Fls. Nº
3690

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
0288
Fls Nº
3690
Doc.

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

202861 J/ETMG_05/

Roteador Tipo 1 doc 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0289
Doc 3690

14.530

Cisco – Software Installation and Upgrade Procedure

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 0290
Doc. 3690

14.509

Table of Contents

Software Installation and Upgrade Procedure **1**
for the 1000, 1400, 1600–R, 1700, 2600, 3600, 3700, 4000, 4500, 4700, AS5300, and the MC3810 1
Introduction 1
Before You Begin 1
Conventions 2
Prerequisites 2
Components Used 2
Upgrade Procedure for Routers with Internal Flash (for example, 2600 Series Routers) 2
Establish a console session to the router 3
Verify that the TFTP server has IP connectivity to the router 4
Copy the new image into the Flash memory of the router through the TFTP server 4
Upgrade Procedure for Cisco 3600 Series Routers with PCMCIA Cards 7
Establish a console session to the router 7
Verify the amount of free space on the Flash memory card (PCMCIA slot) 7
Verify that the TFTP server has IP connectivity to the router 7
Copy the new image into the Flash memory card through the TFTP server 8
Set boot statements to load the new image upon startup 9
Reboot the router to load the new image 10
Verify the upgrade 10
Related Information 11

RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls Nº 0291
Doc 3690

Software Installation and Upgrade Procedure

for the 1000, 1400, 1600–R, 1700, 2600, 3600, 3700, 4000, 4500, 4700, AS5300, and the MC3810

Introduction
Before You Begin
Conventions
Prerequisites
Components Used
Upgrade Procedure for Routers with Internal Flash (for example, 2600 Series Routers)
Establish a console session to the router
Verify that the TFTP server has IP connectivity to the router
Copy the new image into the Flash memory of the router through the TFTP server
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
Related Information

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0292
3690
Doc.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

14.507

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)

POS [illegible]/2005 - CN
CPMI - CORREIOS
0293
Fls. Nº
3690
Doc.

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)>
```

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0294
Doc. 3690

```
device does not contain a valid magic number
boot: cannot open "flash:"
boot: cannot determine first file name on device "flash:"
```

14.505

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
   ```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0295
Doc. 3690

Note: The filename is case sensitive, so be sure to enter it correctly.

4. Specify the destination filename.

JH. 504

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... eeee
```

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"
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0297
Doc. 3690

Upgrade Procedure for Cisco 3600 Series Routers with PCMCIA Cards

14.502

- 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.

ECT nº 03/2005 - CN
CPMI - CORREIOS
0298
Fls Nº
3690

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 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
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0299
3690
Doc.

```
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
```


ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0300
Doc. 3690

```
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#
```

14.499

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
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0301
Doc. 3690

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**

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0302
Doc 3690

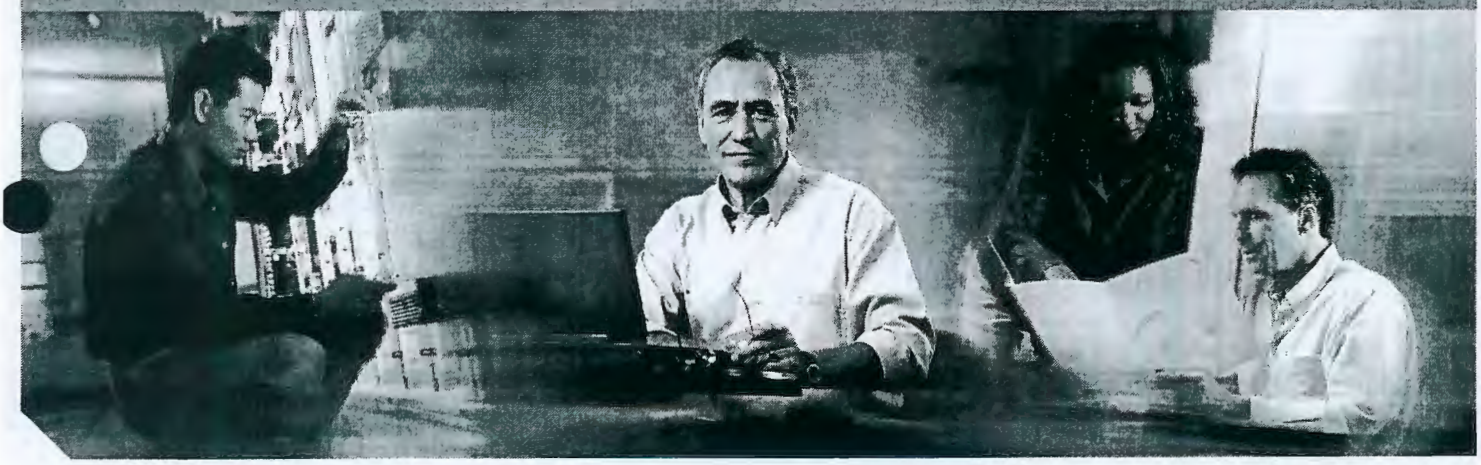
Roteador Tipo 1 doc 6

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0303
3690

Cisco Systems

14.496
J

Quick Start Guide



Cisco 3745 Router

1 Cisco 90-Day Limited Hardware Warranty Terms
2 Documents, Equipment, and Tools
3 Install Chassis
4 Connect Cables
5 Power Up the Router
6 Perform Initial Configuration
7 Interface Numbering
8 Where to Go Next
9 Obtaining Documentation
10 Obtaining Technical Assistance
11 Obtaining Additional Publications and Information

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0304
3690

1 Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranty applicable to Cisco software, is available on the Cisco Documentation CD and on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty document from the CD or from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

   The Warranties and License Agreements page appears.
2. To read the *Cisco Information Packet*, follow these steps:
   a. Click the Information Packet Number field, and make sure that the part number 78-5235-02F0 is highlighted.
   b. Select the language in which you would like to read the document.
   c. Click Go.

      The Cisco Limited Warranty and Software License page from the Information Packet appears.
   d. Read the document online, or click the PDF icon to download and print the document in Adobe Portable Document Format (PDF).

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website, http://www.adobe.com.

3. To read translated and localized warranty information about your product, follow these steps:
   a. Enter this part number in the Warranty Document Number field: 78-5236-01C0
   b. Select the language in which you would like to read the document.
   c. Click Go.

      The Cisco warranty page appears.
   d. Review the document online, or click the PDF icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

http://www.cisco.com/public/Support_root.shtml

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	

POS nº 03/2005 - CN
CPMI - CORREIOS
0305
Fls Nº
3690

2 Documents, Equipment, and Tools

User Documentation

All the documents described here are available online and on the documentation CD-ROM. To be sure of obtaining the latest information, you should access the online documentation.

To view or print a document in its original page format, access the online document, and click on the PDF icon.

For information about accessing user documentation, see the "Where to Go Next" section on page 20.

Items Included with Cisco 3745 Routers

- Rack-mount brackets; ground lug; power cords
- RJ-45-to-DB-9 adapter cable for console connection
- RJ-45-to-DB-25 adapter cable for modem connection
- Ethernet cables for LAN interface (two)
- *Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information* document
- *Cisco 3745 Modular Routers Quick Start Guide* (this document)

Items Not Included

Individual items in this list may be required for your particular application:

- Screws for installing the chassis in a rack
- PC running terminal emulation software for administrative access, or modem for remote administrative access
- Cables for WAN and voice interfaces and for additional LAN interfaces
- Tools: Number 2 Phillips screwdriver; ESD-preventive wrist strap

3 Install Chassis

Safety Information

For safety information you need to know before working on your Cisco router, see the *Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information* document that accompanied this device.

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Warning **To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules (such as power supplies, fans, or cards); these types of handles are not designed to support the weight of the unit.**

CPMI - CORREIOS
0306
Fls. Nº
3690
Doc.

Installing the Chassis

You can set the chassis on a desktop or install it in a rack. See the applicable instructions that follow.

Rack-Mounting the Chassis

The standard accessory kit contains brackets for mounting the chassis in a 19-inch rack. You can order an optional accessory kit with brackets and instructions for mounting the chassis in a 23- or 24-inch rack.

You can mount the chassis in the following ways:

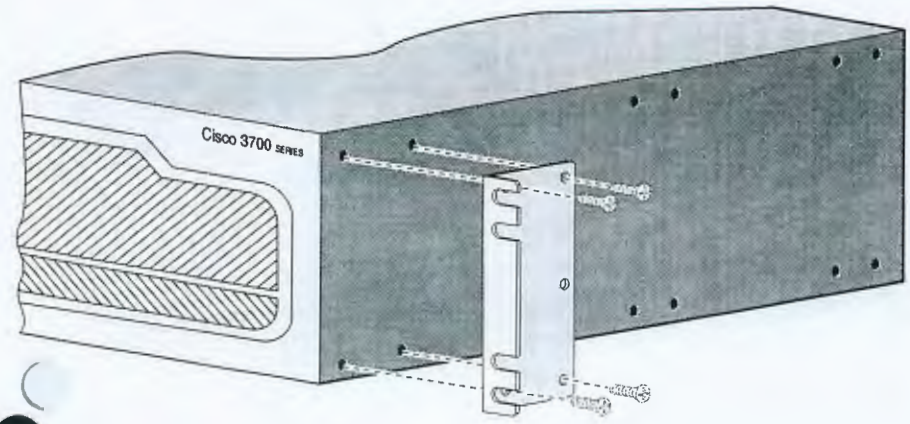
- Front panel forward
- Rear panel forward
- Center mount with either front or rear panel forward

Attaching Brackets

Attach the mounting brackets to the chassis as shown in Figure 1, Figure 2, or Figure 3, using the screws provided in the bracket kit. Attach the second bracket to the opposite side of the chassis. Use a number 2 Phillips screwdriver to install the bracket screws.

Note Some 19-inch racks have power strips on the rear vertical rails that block cable access to power supplies. Be sure to choose an orientation that provides unrestricted access to the rear panel.

Figure 1 Bracket Installation—Front Panel Forward



RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 0307
Doc. 3690

Figure 2 Bracket Installation—Rear Panel Forward

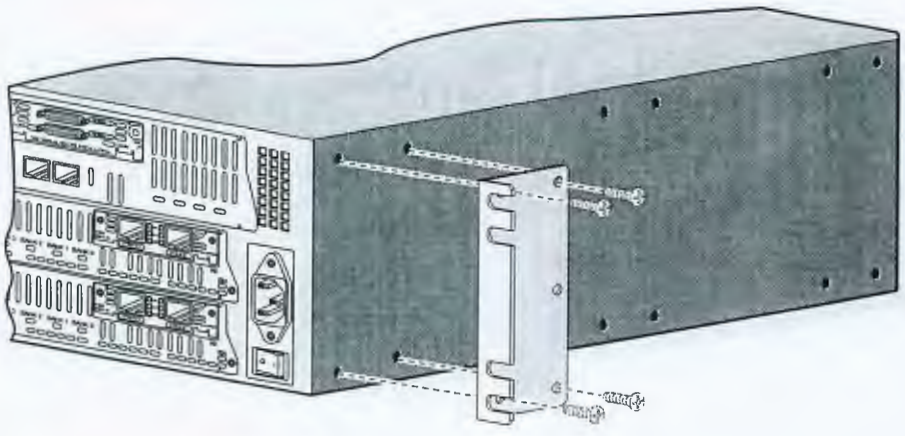
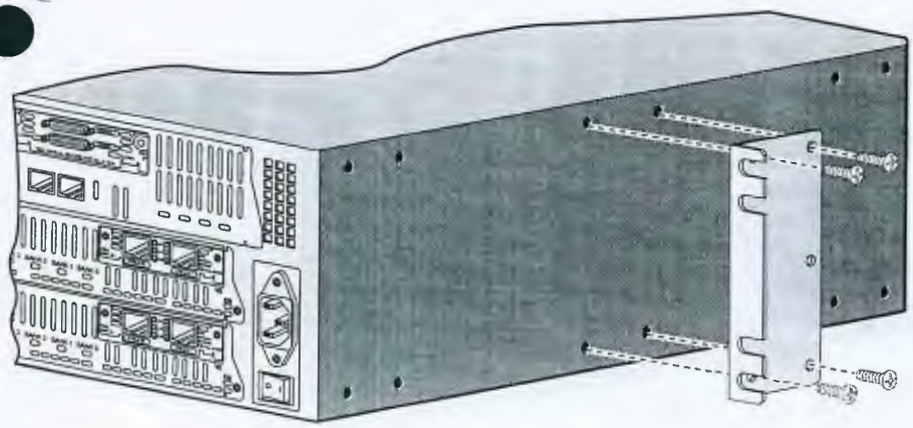


Figure 3 Bracket Installation—Rear Panel Forward, Center-Mount Rack



Note The brackets can also be installed with the front panel forward.

Installing the Chassis in a Rack

Install the chassis in the rack. Rack-mounting screws are not provided with the router. Use two screws for each side (supplied with the rack).

Installing on a Desktop

Caution If you place the Cisco 3745 on a desktop, do not place anything on top of the router that weighs more than 10 pounds (4.5 kg). Excessive weight on top could damage the chassis.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0308
Doc. 3690

Grounding the Chassis

You must connect the chassis to reliable earth ground using the ground lug (provided) and size AWG 6 (13 mm^2) wire.

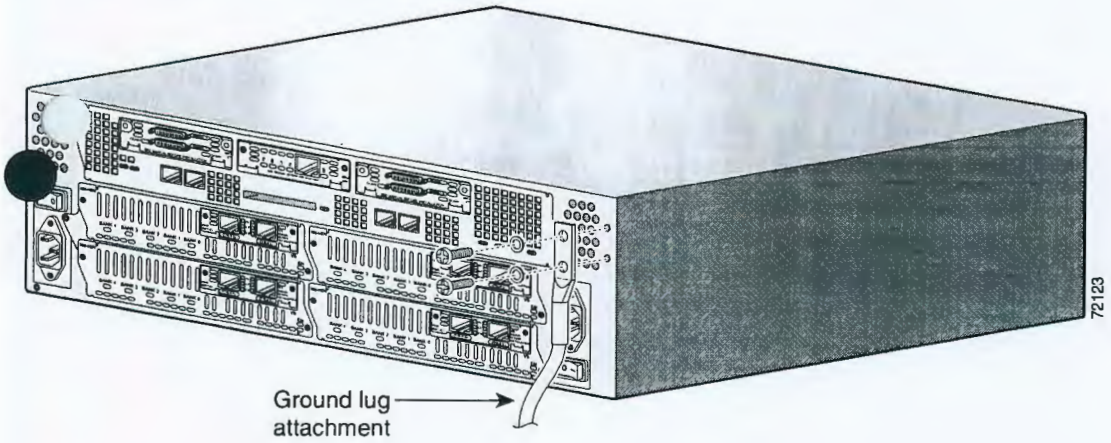
Step 1 Strip one end of the ground wire to expose approximately 0.75 in. (20 mm) of conductor.

Step 2 Use a crimp tool to crimp the ground wire to the ground lug.

Step 3 Attach the ground lug to the chassis as shown in Figure 4. Use a number 2 Phillips screwdriver and the screws supplied with the ground lug. Tighten the screws to a torque of 8 to 10 in-lb (0.9 to 1.1 N-m).

Step 4 Connect the other end of the ground wire to a grounding point at your site.

Figure 4 Required Chassis Ground Connection



4 Connect Cables

Warning **Do not work on the system, or connect or disconnect cables during periods of lightning activity.**

System Management Connections

The connections described in Table 1 provide system management access.

Table 1 System Management Connections

Port	Color	Connected to:	Cable
Console	Light blue	PC or ASCII terminal communication port (usually labeled COM)	RJ-45-to-DB-9 adapter cable
Auxiliary	Black	Modem for remote access	RJ-45-to-DB-25 adapter cable

RQS nº 03/2005 - CN
CPMI - CORREIOS
0309
Fls - Nº
3690
Doc.

Power Connections

Connecting Routers to AC Power

If your router uses AC power, connect it to a 15 A, 120 VAC (10 A, 240 VAC) circuit with overcurrent protection.

Note The input voltage tolerance limits for AC power are 85 and 264 VAC.

Warning **AC connected units must have a permanent ground connection in addition to the power cable ground wire. NEBS-compliant grounding satisfies this requirement.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
15A, 120VAC (10A, 240VAC).

Connecting Routers to DC Power

If your router has a DC-input power supply, follow the directions in this section for proper wiring.

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
20A, 60VDC.

Warning **Use copper conductors only.**

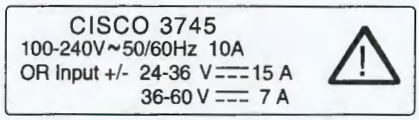
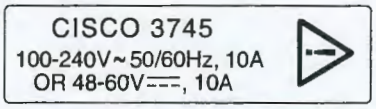
Note The installation must comply with the 1996 National Electric Code (NEC) and other applicable codes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0310
Doc. 3690

DC Wiring Requirements

A Cisco 3745 router with a DC-input power supply requires copper wire for the power connections. Table 2 summarizes the wiring requirements.

Table 2 DC Wiring Requirements for Cisco 3745 Routers

Installed Power Supply	DC Input	DC Input Wire Size	Safety Ground Wire Size	Wire Terminal (Lug)	Overcurrent Protection
Nominal 24/48 VDC[1] Identified by the following printed label: 	24 - 36 V, 15 A	AWG 12 (3.0 mm^2)	AWG 12 (3.0 mm^2), minimum	Amp/Tyco No. 52961 or equivalent	20 A maximum
	36 - 60 V, 7 A	AWG 12 or 14 (3.0 or 2.0 mm^2)	AWG 12 (3.0 mm^2), minimum	For AWG 12: Amp/Tyco No. 52961 or equivalent For AWG 14: Molex No. 19099-0017 or equivalent	20 A maximum
Nominal 48 VDC[2] Identified by the following printed label: 	48 - 60 V, 10 A	AWG 14 or 16 (2.0 or 1.2 mm^2)	AWG 14 (2.0 mm^2), minimum	For AWG 14 or 16: Molex No. 19099-0017 or equivalent	20 A maximum

1. The input voltage tolerance limits for nominal 24/48 V power supplies are 18 and 72 VDC.
2. The input voltage tolerance limits for nominal 48 V power supplies are 38 and 72 VDC.

Wiring Procedure for DC Input

To connect the router to a DC power source, perform the following steps:

Step 1 Remove power from the DC circuit. To ensure that power is removed from the DC circuit, locate the circuit breaker for the DC circuit, switch the circuit breaker to the OFF position, and tape the circuit-breaker switch in the OFF position.

Secure all power cabling when installing this unit to avoid disturbing field-wiring connections.

Step 2 Strip the wires to the appropriate length for the terminals. The strip length is 1/8 to 3/16 inch (3 to 5 mm) for Molex number 19073-0009 terminals and for AMP/Tyco number 52961 terminals.

Step 3 Crimp the terminals onto the DC power input wires.

Warning **When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.**

Step 4 Remove the plastic cover from the terminal block. Save it for reinstallation after you finish wiring.

Step 5 Connect the DC power input wires to the terminal block as shown in Figure 5 or Figure 6.

Caution Do not overtorque the terminal block screws. The recommended torque is 8.0 ± 0.5 in-lb (0.93 ± 0.05 N-m).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0311
Doc: 3690

Figure 5 Terminal Block Connections for Negative Polarity DC Input Power

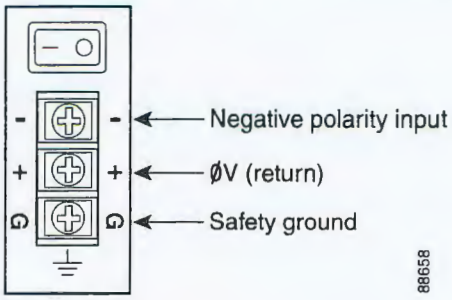
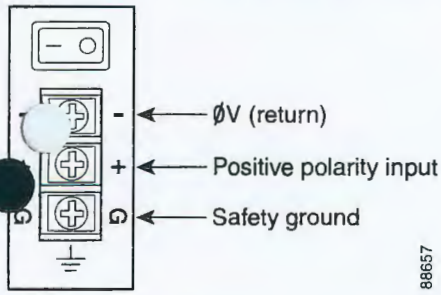


Figure 6 Terminal Block Connections for Positive Polarity DC Input Power



Step 6 Install the plastic cover over the terminal block.

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.**

Step 7 Secure the wires using cable ties.

Step 8 If your router has a second power supply installed, repeat Step 1 through Step 7 for the second power supply.

Step 9 Turn on power to the DC circuit.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0312
Fls. Nº
3690

WAN, LAN, and Voice Connections

The connections and cables listed here are described in detail in the following documents:

- *Cisco 3700 Series Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Cisco Interface Cards Installation Guide*
- *Cisco Modular Access Router Cable Specifications*

For information about accessing these documents, see the "Where to Go Next" section on page 20.

Table 3 summarizes some typical WAN, LAN, and voice connections for Cisco 3745 routers.

Table 3 WAN, LAN, and Voice Connections

Port or Connection	Port Type, Color	Connected to:	Cable
FastEthernet	RJ-45, yellow,	Ethernet hub or switch	Straight-through Ethernet
T1/E1 WAN	RJ-48C/CA81A, blue	T1 or E1 network	RJ-48 T1
Cisco serial	60-pin D-sub	CSU/DSU and serial network or equipment	Cisco serial transition cable that matches the signaling protocol (EIA/TIA-232, EIA/TIA-449, V.35, X.21, or EIA/TIA-530) and the serial port operating mode (DTE or DCE). See the *Cisco Modular Access Router Cable Specifications* document for information about selecting these cables.
Cisco Smart serial	Cisco Smart compact connector, blue	CSU/DSU and serial network or equipment For WIC-2T and WIC-2A/S only	
DSL	RJ-11C/CA11A, lavender	Network demarcation device for service provider's DSL interface	RJ-11
T1 digital voice	RJ-48C/CA81A, tan	Digital PBX	RJ-48 T1 cable
Analog voice FXS	RJ-11, gray	Telephone, fax	RJ-11
Analog voice FXO	RJ-11, pink	Central office, analog PBX	RJ-11
Analog voice E&M	RJ-11, brown	Analog PBX	RJ-11
BRI S/T WAN (external NT1)	RJ-48C/CA81A, red	NT1 device or private integrated network exchange (PINX)	RJ-48
BRI U WAN (built-in NT1)	RJ-49C/CA-A11, orange	ISDN network	RJ-49
CT1/PRI	T1	External T1 CSU	DB-15 T1 serial cable
CT1/PRI-CSU	T1	RJ-48C/CA81A interface	RJ-48 straight-through
CE1/PRI	E1	E1 network	DB-15 to BNC, DB-15 to DB-15, DB-15 to twinax, or DB-15 to RJ-45
56/64-kbps DSU/CSU	8-pin modular, blue	RJ-48S interface	RJ-48 straight-through

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0313
D 3690

5 Power Up the Router

Checklist for Power-Up

You are ready to power on the Cisco router if the following steps are completed:

- The chassis is securely mounted.
- Power and interface cables are connected.
- Your PC terminal emulation program is configured for 9600 baud, 8 data bits, 1 stop bit, and no parity.
- You have selected passwords for access control.
- You have determined the IP addresses for the Ethernet and serial interfaces.

Front Panel Indicators

The following indicator LEDs provide power, activity, and status information:

- YS—System status:
  - Blinking green during boot-up—System is booting
  - Continuous green—System booted and OK
  - Blinking green continuing after boot-up—System is in ROM monitor mode
  - Amber—System malfunction
- ACT—Activity:
  - Blinking or continuous green during system activity, such as interrupts and packet transfers
- SYS PS1 or SYS PS2—Chassis power supply number 1 or number 2 status:
  - Off—Powered off, not installed, or faulty
  - Continuous green—Installed and operating
  - Amber—Installed and powered off or faulty
- -48V PS1 or -48V PS2—IP power module number 1 or number 2 status:
  - Off—Faulty or not installed
  - Continuous green—Installed and operating
  - Amber—Installed and powered off or faulty

Power-Up Procedure

Perform this procedure to power up your Cisco router and verify that it goes through its initialization and self-test. When this procedure is finished, the Cisco router is ready to configure.

Note To view the boot sequence through a terminal session, you must have a console connection to the Cisco router before it powers on.

Move the power switch on the chassis power supply, or on both chassis power supplies, to the ON position.

The fan should operate, and the SYS PS LED should be continuous green for each power supply that is in use. The SYS LED should blink while the system boots, and it should be continuous green after the system boots. If this does not happen, see the power-on procedure in the *Cisco 3700 Series Hardware Installation Guide*.

Note If no Cisco IOS image is loaded on the Cisco 3745, the router enters ROMMON mode, and the system LED blinks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0314
Doc. 3690

Messages begin to appear in your terminal emulation program window.

Caution *Do not press any keys on the keyboard until the messages stop.* Any keys pressed during this time are interpreted as the first command typed when the messages stop, which might cause the router to power off and start over. It takes a few minutes for the messages to stop.

When you see the following messages, the router has booted and is ready for initial configuration. See the following section for initial configuration procedures.

```
        --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Would you like to enter the initial configuration dialog? [yes/no]:
```

Note If the `rommon 1>` prompt appears, your system has booted in ROM monitor mode. For information on the ROM monitor, see the router rebooting and ROM monitor information in the *Cisco IOS Configuration Fundamentals Configuration Guide* for your Cisco IOS software release.

You can access this document at the locations described in the "Where to Go Next" section on page 20.

6 Perform Initial Configuration

You can configure your router by using one of the following tools:

- Setup Command Facility. See the "Initial Configuration Using Setup Command Facility" section on page 12.
- Security Device Manager (SDM). See the "Initial Configuration Using Security Device Manager" section on page 14.
- Command-Line Interface (CLI). See the "Initial Configuration Using the CLI (Manual Configuration)" section on page 17.

Note If you need help with the interface and port numbering, see the "Interface Numbering" section on page 18.

Initial Configuration Using Setup Command Facility

This section shows how to prepare the system for communication functions through its Ethernet and WAN interfaces. For a description of the interface numbering, see the "Interface Numbering" section on page 18.

Note If you make a mistake while using the setup command facility, you can exit and run the facility again. Press Ctrl-c, and type setup at the privileged EXEC mode prompt (`3700#`).

Step 1 To proceed using the setup command facility, enter yes.

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

Step 2 When the following messages appear, press Return to enter basic management setup:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
0315
Fls Nº
3690

```
Would you like to enter basic management setup? [yes/no]: yes
```

Step 3 Enter a host name for the router (this example uses 3745):

```
Configuring global parameters:

  Enter host name [Router]: 3745

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This
password, after entered, becomes encrypted in the configuration.
```

Step 4 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration:

```
Enter enable secret: xxxx

The enable password is used when you do not specify an enable secret password, with some older software
versions, and some boot images.
```

Step 5 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration:

```
Enter enable password: xxxx

The virtual terminal password is used to protect access to the router over a network interface.
```

Step 6 Enter the virtual terminal password, which prevents unauthenticated access to the router through ports other than the console port:

```
Enter virtual terminal password: xxxx
```

Step 7 Respond to the following prompts as appropriate for your network:

```
Configure SNMP Network Management? [yes]: yes
    Community string [public]:
```

Step 8 A summary of the available interfaces is displayed:

Note The interface numbering that appears is dependent on the type of Cisco modular router platform and on the installed interface modules and cards.

```
Current interface summary

Controller Timeslots D-Channel Configurable modes Status
T1 3/0     24         23        pri/channelized    Administratively up
T1 3/1     24         23        pri/channelized    Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      NO  unset  up                    down

FastEthernet0/1            unassigned      NO  unset  up                    down
```

Step 9 Select one of the available interfaces for connecting the router to the management network:

```
Enter interface name used to connect to the
management network from the above interface summary: fastethernet0/0
```

Step 10 Respond to the following prompts as appropriate for your network:

```
Configuring interface FastEthernet0/0:
  Use the 100 Base-TX (RJ-45) connector? [yes]:
  Operate in full-duplex mode? [no]: yes
  Configure IP on this interface? [yes]:
    IP address for this interface: 10.1.1.1
    Subnet mask for this interface [255.0.0.0] : 255.255.0.0
    Class A network is 10.0.0.0, 16 subnet bits; mask is /16
```

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0316
Doc 3690

14.483
3

Step 11 After the following messages appear, press Return to save the basic configuration:

```
The following configuration command script was created:

hostname 3745
enable secret 5 $1$Ksjf$za4T21b3ARS5d1PHVzW5A0
enable password xxxx
line vty 0 4
password xxxx
snmp-server community public
!
no ip routing

!
interface FastEthernet0/0
no shutdown
media-type 100BaseX
full-duplex
ip address 10.1.1.1 255.255.0.0
!
interface FastEthernet0/1
shutdown
no ip address
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2


Press RETURN to get started! RETURN
```

Step 12 The user prompt is displayed.

```
3745>
```

When you have completed the basic configuration tasks, your Cisco router is ready to configure for specific functions. See the "Where to Go Next" section on page 20 for information about locating documentation for advanced configuration procedures.

itial Configuration Using Security Device Manager

Security Device Manager (SDM) is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, Network Address Translation (NAT), firewalls, Virtual Private Networks (VPNs), and other features on your router. SDM runs on a PC connected to the router through an Ethernet or FastEthernet interface, and it requires a web browser, either Internet Explorer version 5.5 or later or Netscape version 4.79. SDM is compatible with Microsoft Windows 2000, Windows NT 4.0 (with Service Pack 4), Windows 98, Windows ME, and Microsoft Windows XP.

This procedure applies to routers that have the SDM configuration tool preinstalled.

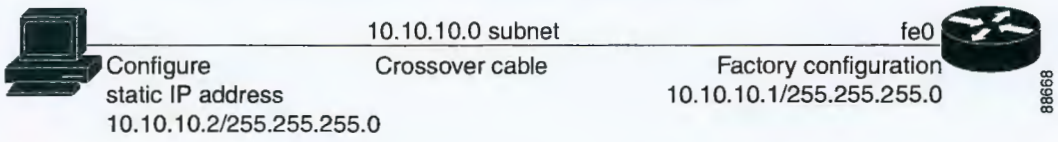
To configure your router by using SDM, first assign an IP address to the Ethernet port of the PC as directed in the "Assign a Static IP Address to the PC" section, and then start SDM as described in the "Start SDM" section on page 15.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0317
3690

Assign a Static IP Address to the PC

Assign a static IP address in the 10.10.10.0 subnet to the Ethernet port of the PC, as shown in Figure 7. The recommended IP address for this interface is 10.10.10.2. The FastEthernet 0/0 interface of the router is preconfigured with the IP address 10.10.10.1.

Figure 7 Initial IP Addresses in the 10.10.10.0 Subnet for SDM



Start SDM

To start SDM and begin the router configuration, perform the following procedure:

Step 1 Connect the Ethernet port of the PC to the FastEthernet 0/0 port of the router, using a crossover cable.

Step 2 Open a web browser on the PC, and enter the following URL:

https://10.10.10.1/flash/sdm.shtml

Note https://... specifies that the Secure Socket Layer (SSL) protocol is used for a secure connection. If SSL is not available, you can use http://... .

Step 3 Enter the username sdm and the password sdm in the dialog box.

Step 4 A window appears informing you that Verisign certifies that this is a Cisco application. Click Yes, or click Grant to accept the certificate and proceed. Additional certificate windows appear if you are using Netscape; click Grant to accept the certificates.

The SDM Launch page appears after a short time. (See Figure 8.) Leave this window open and wait for the next window.

Figure 8 SDM Launch Page

RUS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0318
Doc 3690

Tip If the SDM Launch page does not appear when you enter the URL https://10.10.10.1/flash/sdm.shtml, test the connection between the PC and the router by doing the following:

a. Check that the POWER LED on the router is on and that the ACTIVITY LED is on, indicating an active Ethernet connection between the router and the PC. If the ACTIVITY LED is not on, verify that you are using a crossover cable to connect the PC to the router.

b. If the Launch page still does not appear, verify that the web browser's "work offline" option is disabled. In Internet Explorer, click the File menu, and verify that the "work offline" option is unchecked. In Netscape, the default selection in the File menu is set to "work online."

c. If the Launch page still does not appear, verify that the file sdm.tar is loaded into the router's Flash memory. Open a Telnet session to 10.10.10.1, entering the username sdm and the password sdm. Enter the command show flash to verify that sdm.tar is loaded in Flash memory.

d. If the web page still does not appear, verify that the PC is configured with a static IP address.

Step 5 A window appears with information about the web browser and its settings. This window also informs you that SDM will open in another window. Close this window and wait for the SDM Startup Wizard page to appear.

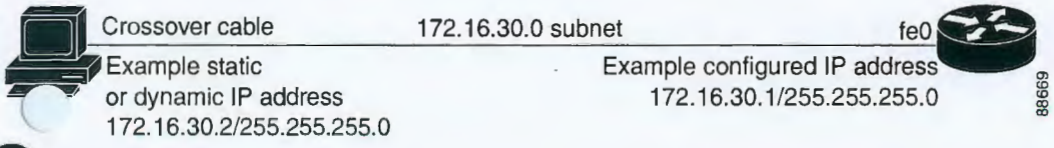
Step 6 When the SDM Startup wizard appears, click Next to begin. Use the wizard to give the router a hostname, to assign a login username and password, to set an enable secret password, and to assign a new LAN IP address to the FastEthernet interface 0/0. You can also configure the router as a Dynamic Host Configuration Protocol (DHCP) server, identify Domain Name System (DNS) and Windows Internet Naming Service (WINS) servers, and make security settings.

Tip Be sure to write down the enable secret password. It is not revealed in the summary window and cannot be recovered.

Step 7 When the Summary window appears, write down the LAN IP address, hostname, login username, and user password that you entered, and click Finish. (You will need this information to reconnect to the router and use SDM to perform additional configuration.)

Step 8 Assign a new IP address to the PC's Ethernet interface; place it on the same subnet as the router's FastEthernet 0/0 port, which you assigned in Step 6 above. (See Figure 9.) If you configured a DHCP server on the router, configure the PC to obtain an IP address automatically. The IP addresses in Figure 9 are examples only.

Figure 9 IP Addresses in the Renumbered Subnet for SDM



Step 9 Open a web browser on the PC, and enter the SDM URL, using the new IP address that you gave the LAN interface: https://*new-IP-address*/flash/sdm.shtml. In the example shown in Figure 9, you would enter `https://172.16.30.1/flash/sdm.shtml`.

Step 10 Enter the username and password that you specified in Step 6 above.

Step 11 When the SDM System Overview window appears, you can use the wizard buttons on the left side of the window to configure other features. Buttons are provided for LAN, WAN, firewall, and VPN configurations.

For more information about SDM, refer to the *Cisco Security Device Manager Troubleshooting Guide* at the following URL, http://www.cisco.com/go/sdm. See the "Obtaining Documentation" section on page 20 for information about accessing this document.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0319
Doc. 3690

Initial Configuration Using the CLI (Manual Configuration)

This section shows how to bring up a command-line interface (CLI) prompt for configuration using the CLI, and it directs you to the documentation for CLI configuration.

Note To avoid losing work you have completed, be sure to save your configuration occasionally as you proceed. Use the copy running-config startup-config command to save the configuration to NVRAM.

Step 1 To proceed with manual configuration using the CLI, enter no.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 2 Press Return to terminate autoinstall and continue with manual configuration.

```
Would you like to terminate autoinstall? [yes] Return
```

Several messages are displayed, ending with a line similar to the following:

```
...
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled date time by person
```

Step 3 Press Return to bring up the `Router>` prompt.

```
...
flashfs[4]: Initialization complete.
Router>
```

Step 4 Enter privileged EXEC mode.

```
Router> enable
Router#
```

For configuration using the CLI, refer to the applicable configuration procedures in the *Software Configuration Guide: Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*. See the "Where to Go Next" section on page 20 for information about accessing this document.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0320
3690

7 Interface Numbering

Each individual interface (port) on a Cisco 3745 router is identified by number as described in the following sections.

WAN and LAN Interface Numbering

The Cisco 3745 router chassis contains the following WAN and LAN interface types:

- 2 built-in FastEthernet LAN interfaces
- 3 slots in which you can install WAN or voice interface cards
- 4 network module slots

The numbering format is:

- *Interface-type Slot-number/Interface-number*

  Two examples are: `FastEthernet 0/0` and `Serial 1/2`.

The slot numbers are as follows:

- 0 for all built-in interfaces
- for all WIC interfaces
- 1 for the lower-right network module slot
- 2 for the lower-left network module slot
- 3 for the upper-right network module slot
- 4 for the upper-left network module slot

If double-width network modules are installed, the network module slots are numbered as follows:

- 2 for the lower double-width slot
- 4 for the upper double-width slot

Interface (port) numbers begin at 0 for each interface type, and continue from right to left and from bottom to top.

Figure 10 shows the rear panel of the Cisco 3745 with:

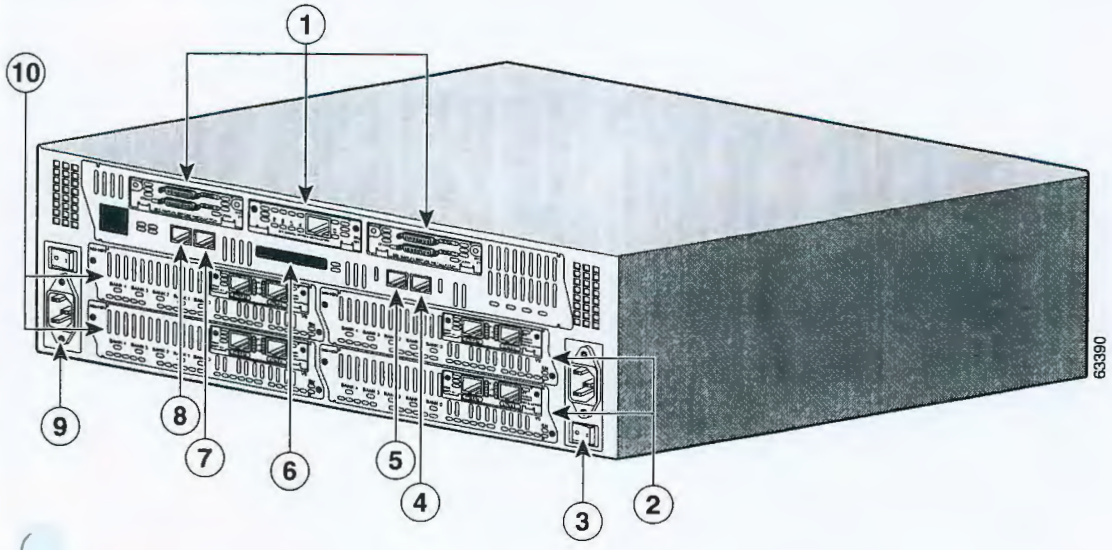
- A WIC in each of the three WAN interface card slots
- A single-width network module in each of the four network module slots
- Two AC power supplies

Note The slot number for all WIC interfaces is always 0. (The W0, W1, and W2 slot designations are for physical slot identification only.) Interfaces in the WICs are numbered from right to left, starting with 0/0 for each interface type, regardless of which physical slot the WICs are installed in. Some examples are:

- If physical slot W0 is empty and physical slot W1 contains a 1-port serial WIC, the serial interface in the WIC is numbered Serial 0/0.
- If slot W0 contains a 2-port serial WIC and slot W1 contains a 1-port serial WIC, the serial interfaces in physical slot W0 are numbered Serial 0/0 and Serial 0/1, and the serial interface in physical slot W1 is numbered Serial 0/2.
- If slot W0 contains a 2-port serial WIC and slot W1 contains a 1-port BRI WIC, the serial interfaces in physical slot W0 are numbered Serial 0/0 and Serial 0/1, and the BRI interface in physical slot W1 is numbered BRI 0/0.

RC 3 nº 03/2005 - CN
CPMI - CORREIOS
0321
Fls. Nº
3690
Doc.

Figure 10 Cisco 3745 Rear Panel



	Interface card slots	6	Cisco 3700 Compact Flash slot
2	Network modules	7	Auxiliary port
3	Power supply	8	Console port
4	FastEthernet 0/0	9	Power supply
5	FastEthernet 0/1	10	Network modules

Voice Interface Numbering

Voice interfaces are numbered differently from the WAN interfaces described in the previous section. Voice interfaces are numbered as follows:

network-module-slot/voice-module-slot/voice-interface

If a 4-channel voice network module is installed in chassis slot 1, the voice interfaces are:

- 1/0/0—Network module slot 1/Voice module slot 0/Voice interface 0
- 1/0/1—Network module slot 1/Voice module slot 0/Voice interface 1
- 1/1/0—Network module slot 1/Voice module slot 1/Voice interface 0
- 1/1/1—Network module slot 1/Voice module slot 1/Voice interface 1

Fls Nº 0322
3690

8 Where to Go Next

For additional detailed configuration procedures, refer to the appropriate Cisco 3700 series documentation or Cisco IOS software documentation, available on-line and on the Documentation CD-ROM:

Tip See the "Obtaining Documentation" section on page 20 for help in locating these documents.

To access Cisco 3700 series platform documentation on Cisco Connection Online (CCO):

On the Cisco.com home page at http://www.cisco.com, locate the Technical Documentation tab, and click on "Locate Technical Documentation on Cisco Connection Online." Under the Product Documentation heading, navigate to Modular Access Routers and to the documentation for your router.

To access Cisco IOS software documentation on Cisco Connection Online (CCO):

On the Cisco.com home page at http://www.cisco.com, locate the Technical Documentation tab, and click on "Locate Technical Documentation on Cisco Connection Online." Under the Product Documentation heading, navigate to the Cisco IOS software documentation for the Cisco IOS software release that is installed on your router.

To access documentation on Cisco.com:

For Cisco 3700 series platform documentation, start on Cisco.com at http://www.cisco.com, and select Products & Services > Routers > Cisco 3700 Series Multiservice Platforms > Technical Documentation > *Document type* > *Document*.

For Cisco IOS software documentation, start on Cisco.com at http://www.cisco.com, and select Products & Services > IOS Software > Cisco IOS Software Releases > *Your Cisco IOS software release*.

To get updated information about platform support for features, select Feature Navigator II, if you have an account on Cisco.com. You can also access Feature Navigator II at http://www.cisco.com/go/fn.

9 Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 3690
Doc.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click Feedback at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

10 Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0324
Doc. 3690

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

RCS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0325
Doc. 3690

11 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0326
3690
Doc.

JU.473
J

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc. Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet* PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Printed in the USA on recycled paper containing 10% postconsumer waste

78-13503-04

DOC 7813503=

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0327
Doc. 3690

14.472
J

Roteador Tipo 1 doc 7

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0328
Doc. 3690

Release Notes For Security Device Manager Version 1.0

6/27/03

These release notes support Security Device Manager 1.0. These release notes should be used with the documents listed in the related documentation section. These release notes are updated as needed.

Contents

This document contains the following sections:

- Introduction, page 1
- System Requirements, page 2
- Installation Notes, page 5
- Important Notes, page 6
- Caveats, page 8
- Documentation Updates, page 13
- Related Documentation, page 15
- Obtaining Documentation, page 15
- Obtaining Technical Assistance, page 16
- Obtaining Additional Publications and Information, page 18

Introduction

Security Device Manager (SDM) is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, Network Address Translation (NAT), firewalls, Virtual Private Networks (VPNs), and other features on your router. SDM is installed in router Flash memory, and is run in a Web browser installed on a PC. SDM may be preinstalled on the routers listed in the "Hardware Supported" section on page 2.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0329
Doc. 3690

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

System Requirements

This section contains SDM system requirements.

Memory Requirements

SDM requires 2.3 MB of free Flash memory space on supported routers.

Hardware Supported

This section lists the hardware that SDM supports.

Cisco Routers

SDM is supported on the following Cisco 800 series routers:

- Cisco 831
- Cisco 836
- Cisco 837

SDM is supported on the following Cisco 1700 series routers:

- Cisco 1701
- Cisco 1710
- Cisco 1711
- Cisco 1712
- Cisco 1721
- Cisco 1751
- Cisco 1751-v
- Cisco 1760
- Cisco 1760-v

SDM is supported on the following Cisco 2600 series routers:

- Cisco 2610XM
- Cisco 2611XM
- Cisco 2620XM
- Cisco 2621XM
- Cisco 2650XM
- Cisco 2651XM
- Cisco 2691

SDM is supported on the following Cisco 3600 series routers:

- Cisco 3620
- Cisco 3640

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0330
Doc. 3690

- Cisco 3640A
- Cisco 3661
- Cisco 3662

SDM is supported on the following Cisco 3700 series routers:

- Cisco 3725
- Cisco 3745

Network Modules and WICs Supported

SDM supports configuration on following Network Modules.

- NM-1E
- NM-4E
- NM-4T
- NM-2W
- NM-1E2W
- NM-1FE2W
- NM-2E2W
- NM-2FE2W
- NM-1FE-FX
- NM-1FE-TX
- NM-4A/S (synchronous only)
- NM-8A/S (synchronous only)

SDM supports only Ethernet configuration on following NMs

- NM-1E1R2W
- NM-1FE1R2W
- NM-1FE1CE1U
- NM-1FE2CE1B
- NM-1FE1CE1B
- NM-1FE2CE1U
- NM-1FE1CT1
- NM-1FE2CT1
- NM-1FE1CT1-CSU
- NM-1FE2CT1-CSU

SDM supports the following WAN interface cards:

- WIC-1T
- WIC-2T
- WIC-2A/S (Frame Relay, PPP, HDLC, no async)
- WIC-1DSU-T1

ROS nº 03/2005 - CN
CPMI - CORREIOS
0331
Fls Nº
3690

14,468

- WIC-1ADSL
- WIC-1ENET
- WIC-1SHDSL
- WIC-1DSU-T1-V2

PC System Requirements

SDM is designed to run on a personal computer that has a Pentium III processor.

Software Supported

This section describes SDM software requirements.

Cisco IOS Images

SDM is compatible with the Cisco IOS images listed in Table 1.

Table 1 SDM-Supported Routers and Cisco IOS Versions

SDM-Supported Routers	SDM-Supported Cisco IOS Versions
Cisco 831, 836, and 837	12.2(13)ZH or later.
1701, 1710, 1721, 1751, 1751-v, 1760, and 1760-v	• 12.2(13)ZH, or later • 12.2(13)T3 or later • 12.3(1)M or later • 12.2(11)T6 not supported
1711, 1712	• 12.2(15)ZL or later.
Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, and 2691	• 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 not supported[1] • 12.2(15)ZJ
Cisco 3620, 3640, 3640A, 3661, and 3662	• 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 not supported[1]
Cisco 3725 and 3745	• 12.2(11)T6 or later • 12.3(1)M or later • 12.2(13)T3 not supported[1]

1. 12.2(13)T3 will be supported in the next release of SDM, which will be available in September of 2003.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0332
Doc. 3690

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0333
Doc. 3690

14.467

Determining the Cisco IOS Software Version

To determine the version of Cisco IOS software currently running on your Cisco 820 series router, log in to the router and enter the show version EXEC command. The following sample output from the show version command indicates the version number on the second output line:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (c1700-k8sv3y7-mz) Version 12.2(13)ZH
```

Web Browser Versions

SDM can be used with the following browsers:

- Netscape version 4.79
- Internet Explorer version 5.5 and later.

C Operating System Versions

SDM can be run on a PC running any of the following operating systems:

- Windows NT 4.0 with Service Pack 4.
- Windows 98 (second edition)
- Windows 2000
- Windows ME
- Windows XP

Installation Notes

This section contains important information regarding installation and upgrades to SDM.

Downloading SDM From Cisco.com and Installing It On Your Router

The document *Downloading and Installing Cisco Security Device Manager (SDM) Version 1.0* explains how to download SDM from Cisco.com and install it on your router. To obtain this document, visit the following URL.

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

Upgrading to a New SDM Release

If SDM is already installed on a router, and you are upgrading to a newer SDM release, you must also upgrade the configuration file for the router in order for new SDM software to function properly. The latest SDM configuration files are contained in the SDM .zip file, available from Cisco.com at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/sdm

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0334
3690

J4.466
J

The document *Downloading and Installing Cisco Security Device Manager (SDM) Version 1.0* explains how to obtain the SDM zip file and how to install SDM and all related files on your router. This document is available at the following URL:

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

Uninstalling SDM Files

If you want to remove SDM from Flash memory, you can do so by logging onto your router and completing the following steps in EXEC mode:

Step 1 Type the following commands:

```
router#delete sdm.tar
Delete filename [sdm.tar]?
Delete flash:sdm.tar? [confirm]
router#squeeze flash:
```

Step 2 Repeat the commands to delete the following additional files from Flash memory: sdm.shtml, sdmconfig-*<model>*xxx.cfg. sdmconfig-*<model>*xxx.cfg represents the default configuration file that is supplied with SDM. For example, the default configuration file for the supported 2600 platforms is sdmconfig-26xx.cfg.

Important Notes

This section contains important information for this release.

Routers Shipped with SDM Do Not Execute the Standard IOS Startup Sequence

Because a default configuration file is provided on a router shipped with SDM, it will not execute the standard Cisco IOS startup sequence. If you are expecting to use the Cisco IOS setup utility, a TFTP/BOOTP configuration download, or other features available through the standard Cisco IOS startup, you will need to erase the configuration file.

To erase the existing configuration and take advantage of the Cisco IOS startup sequence, perform the following steps. This will leave SDM on the router if you later decide you want to use it, but you will need to configure the router manually before you can begin using SDM. Please refer to your router's Quick Start Guide and to the SDM FAQ (available at http://www.cisco.com/go/sdm) for information about the minimum configuration required for using SDM.

Step 1 Connect the light blue console cable, included with your router, from the blue console port on your router to a serial port on your PC. Refer to your router's Hardware Installation Guide for instructions.

Step 2 Connect the power supply to your router, plug the power supply into a power outlet, and turn on your router. Refer to your router's Quick Start Guide for instructions.

Step 3 Use a terminal emulation program on your PC, with the terminal emulation settings 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control, to connect to your router.

Step 4 At the prompt, enter the **enable** command, and enter the password **sdm**.

CPMI - CORREIOS
0335
Fls. Nº
3690

```
yourname> enable

Password: sdm
yourname#
```

Step 5 Enter the **erase startup-config** command.

```
yourname# erase startup-config
```

Step 6 Confirm the command by pressing **Enter**.

Step 7 Enter the **reload** command.

```
yourname# reload
```

Step 8 Confirm the command by pressing **Enter**.

After the router completes the reload operation, it enters into the standard IOS startup sequence. You can use the startup sequence to give your router a configuration manually, or to copy a configuration file from the network. If you later decide you want to use SDM to change an existing configuration, refer to the instructions on starting SDM included in the Quick Start Guide for your router.

Unable to perform 'squeeze flash'

If your router is using a Cisco IOS image with a version earlier than 12.3 in the T release, or 12.2(13)ZH, it may be necessary to use the **squeeze flash** command to reclaim Flash memory after repeated use of SDM. If this becomes necessary, SDM will inform you that the **squeeze flash** command must be used, and will execute the command upon your confirmation.

However, the **squeeze flash** command will not work if an **erase flash** command has never been executed on the router. If this is the case you will receive an "Unable to perform 'squeeze flash'" warning message, and you will need to run the erase flash: command to enable the use of the **squeeze flash** command.

Executing the **erase flash:** command will remove SDM and the Cisco IOS image from the router's Flash memory, and you will lose your connection to the router. Complete the following steps to save files in Flash, execute **erase flash:**, and copy the files back so you can reconnect to SDM.

Step 1 Ensure that the router will not lose power. If the router loses power after an **erase flash:** operation, there will be no Cisco IOS image in memory.

Step 2 Prepare a TFTP server to which you can save files and copy them over to the router. You must have write access to the TFTP server. Your PC can be used for this purpose if it has a TFTP server program.

Step 3 Open up a Telnet session on the router so that you can use the CLI.

Step 4 Save the router's running configuration to the startup configuration by entering the command **copy running-config startup-config**.

Step 5 Use the **tftpcopy** command to copy the Cisco IOS image, the file SDM.tar, and the file SDM.shtml from Flash to a TFTP server:

copy flash: *filename* **tftp:**//*tftp-server-address/filename*

Example:

```
copy flash: sdm.tar tftp://10.10.10.3/SDM.tar
```

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0336
Doc 3690

14.469

Note If you prefer to download a Cisco IOS image, the file SDM.tar, and the file SDM.shtml, follow these instructions to use an Internet connection to download an SDM-supported Cisco IOS image, the files SDM.tar, and the file SDM.shtml, then place those files on a TFTP server.

a. Click the following link to obtain a Cisco IOS image from the Cisco Software Center:

   http://www.cisco.com/kobayashi/sw-center/

b. Obtain an image that supports the features you want on the 12.2(11)T release or later. Save the file to the TFTP server that is accessible from the router.

c. Use the following link to obtain the files SDM.tar and SDM.shtml, then save SDM.tar and SDM.shtml to the TFTP server.

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

Step 6 From the PC, log onto the router using telnet, and enter Enable mode.

Step 7 Enter the command **erase flash:**, and confirm. The router's IOS image, configuration file, the file SDM.tar, and the file SDM.shtml are removed from Flash memory.

Step 8 Use the **tftpcopy** command to copy the IOS image and SDM.tar from the TFTP server to the router:

copy tftp://*tftp-server-address/filename* **flash:**

Example:

```
copy tftp://10.10.10.3/SDM.tar flash:
```

Note Copy the Cisco IOS image first, followed by the files sdm.tar and sdm.shtml.

Step 9 Start your web browser, and reconnect to SDM, using the same IP address you used when you started the SDM session.

Now that an **erase flash:** has been performed on the router, you will be able to execute the squeeze flash command when necessary.

Caveats

Caveats describe unexpected behavior in SDM. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Open Caveats - Release 1.0

This section lists caveats that are open in release 1.0.

- CSCea60147

  SDM client is launched with null pointer exception reported in the Java Console window.

  Workaround

  None necessary.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0337
Doc. 3690

- CSCea71480

  The number of open GRE-over-IPSec tunnels shown in the SDM Monitor Mode Overview window is incorrect.

  Workaround

  None necessary.

- CSCea84865

  In routers running a Cisco IOS image of version 12.2(11)T6, SDM treats PPPoE connections that do not contain the **vpdn-enable**, **vpdn-group, request-dialin,** and **protocol pppoe** commands as read only. The Edit button is not enabled in the Interfaces and Connections window, and the connection is treated as "Other" in the WAN window.

  If SDM is subsequently used to configure another PPPoE connection on the router, those commands are added, and the original PPPoE connections are made complete. However SDM will not show these original connections as editable.

  Workaround

  Select **Refresh** from the View menu to make SDM display these PPPoE connections as editable.

- CSCea89141

  Port Address Translation (PAT) rules configured with no access list using the CLI are not removed when using SDM to delete WAN connections the rules are associated with.

  Workaround

  Remove the PAT rules using the CLI.

- CSCin40086

  SDM can take more than 30 seconds to switch from Advanced Mode to Wizard Mode.

- CSCin42927

  When performing Security Audit from a PC with more than one Network Interface Card (NIC) which is in one of the directly connected Inside Interface networks (as chosen by the user), "Access class not set on VTY lines" security problem as reported cannot be fixed.

- CSCea89451

  By default, the Startup wizard is invoked when the interface that the PC connects to is one of the following: Ethernet 0, Fast Ethernet 0/0, or Fast Ethernet 0. If the router doesn't have any of the listed interfaces, the Startup wizard will not be invoked because the IP address assignment of 10.10.10.1 fails.

  Workaround

  Check the default configuration file on the router. If the router interface you are connecting your PC to on initial startup is not the interface assigned the address 10.10.10.1 in the default configuration file, than either edit the default configuration file to give the interface you are connecting to an IP address and subnet mask, or connect the PC to a network module in Slot0.

- CSCea90231

  Router does not reload with default configuration when user executes Reset To Factory Defaults in SDM.

  If router is running a Cisco IOS image of version 12.2(11)T6, and the last 4 bits of the config-register value are set to 0, for example 0x2100 or 0x1100, the router does not reload when the user performs a Reset To Factory Defaults. SDM indicates that it has sent a **reload** command to router and shuts

ROS nº 03/2005 - CN
CPMI - CORREIOS
0338
3690

14.462

down, and the default configuration is copied to the startup-config, but the **reload** command has not executed, and the router is still using the running configuration that was present before the Reset operation.

Workaround

Use the CLI **config-register** command to ensure that the last 4 bits of the config register are not set to 0 (zero).

- CSCin33529

  SDM may require up to 10 seconds when being run using Internet Explorer version 6.0 with service pack 1 and JRE version 1.4.1_01 to configure a new serial WAN connection in Wizard mode.

- CSCin40379

  Text display is cut and scrolling causes loss of text in Security Audit when browser uses the Java Runtime Environment (JRE) 1.3.1_07 plug-in.

  Various text messages are cut and not displayed properly in the Security Audit feature if JRE 1.3.1_07 is installed on the system. For example, the report card contains incomplete sentences, and scrolling up and down in the "Fix It" window causes many of the lines to disappear or to appear incomplete.

  The problem is seen only when the plug-in is installed.

  Workaround

  Upgrade Java Plugins to the latest version available from the Sun website at the following URL:

  http://java.sun.com/

  Alternatively, disable the Java plugin. In Internet Explorer, click **Tools**, select **Internet Options**, click Advanced, and uncheck the **Use Java 2 v1.3.1_07** option. In Netscape, click **Edit**, select **Preferences**, click **Advanced**, and uncheck **Enable Java Plugin**.

- CSCin42585

  If a user selects Save Running Config to PC from the SDM file menu on a router running a Cisco IOS image of version 12.2(13)ZH or version 12.2(11)T2, the file may not be saved to the PC.

  Workaround

  Shut down SDM and thenrestart it. Then, select the Save Running Config to PC option again, and specify a file name on the PC.

- CSCea89054

  If you delete a WAN connection that you created in Wizard mode, an **ip nat inside** command may still remain in a LAN interface configuration.

  Workaround

  To delete the **ip nat inside** command from the LAN interface configuration, go to Interfaces and Connections in Advanced Mode, select the LAN interface, click Edit, and delete the association in the Association tab.

- CSCin44264

  Enabling AES encryption or IP Compression in the Add/Edit IKE Policy or Add/Edit Transform Set windows might not work even though the IOS image running on the router supports AES encryption o IP Compression. This may happen in the following circumstances:

  - Hardware encryption is enabled.
  - The router has a VPN module that does not support AES encryption or IP compression.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0339
3690
Doc.

Workaround

Do one of the following:

- Disable hardware encryption by adding the **no crypto engine accelerator** command to the configuration file using the CLI interface. This command tells router to use IOS software for encryption instead of using the encryption provided by the VPN module.
- Upgrade your hardware VPN module to one that supports AES or IP Compression.

  For more info on VPN Modules, refer to the document at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet09186a0080088750.html

- CSCeb01244

  In Advanced Mode Static Routing, if a virtual-template interface is configured as the next hop interface in a static route, SDM generates corresponding CLI commands. Delivering such commands to the router may fail on some platforms.

  Workaround

  Do not configure a virtual-template interface as a next hop interface if it is not supported on your router.

- CSCea80627

  After the SDM Startup Wizard has been completed by the user, SDM terminates and all browser windows close except the browser window hosting the Applet area, when run in Netscape Communicator version 4.79.

  Workaround

  Manually close the browser window(s) that remain open.

- CSCea45637

  When SDM is run in a browser using Sun Microsystem's Java Plug-in version 1.4.0, null-pointer exceptions are displayed in the Java console window when SDM loads and starts.

  This problem has been reported by many other users. Refer to the following links for more information:

  http://search.java.sun.com/search/java/index.jsp?qp=&nh=100&qt=CertificateHostnameVerifier&x=32&y=16&col=java&col=javabugs&col=javaforums&col=wireless

  http://forum.java.sun.com/thread.jsp?forum=30&thread=291011

  http://forum.java.sun.com/thread.jsp?forum=2&thread=289203

  Workaround

  Upgrade Java Plugins to the latest version available from the Sun website at the following URL:

  http://java.sun.com/

- CSCdy80223

  When SDM runs with a Cisco IOS image of a version earlier than 12.3 in the T release, or earlier than version 12.2(13)ZH, the HTTP server appends unnecessary characters to names of files it displays. As a result, when SDM is started, the web browser displays the warning "Content does not match the signature."

  Workaround

  Disregard the warning and click **Yes** to continue.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0340
3690

14.460

- CSCin44119

  When an Easy VPN tunnel is active, using SDM to apply a NAT configuration to the Easy VPN inside and outside interfaces will deliver '**ip nat inside**' and '**ip nat outside**' commands to the router, but the running configuration will not be changed. SDM displays no error message when this is attempted.

  Workaround

  To apply a NAT configuration to interfaces that have been designated as Easy VPN "inside" or "outside" interfaces, complete the following steps in SDM:

  - Select the Easy VPN tunnel in the VPN Connections window and click **Disconnect**. If the Connect/Disconnect button is disabled, select the interface in the Interfaces and Connections window, open the Association tab for that connection and change the Easy VPN association to **None**.
  - Open the NAT window, click Designate **NAT Interfaces**, and designate NAT inside and NAT outside interfaces.
  - Select the Easy VPN tunnel, and click **Connect**.. If you had to disassociate the Easy VPN tunnel from the connection, return to the Associations tab, and reselect the Easy VPN connection name

- CSCeb05125

  When SDM is run in Internet Explorer using Java Plugin 1.3.1_07, some text in the Wizard Mode Reset to Factory Defaults screen gets cut off.

  Workaround

  Resize the SDM window to display all text.Upgrade Java Plugins to the latest version available from the Sun website at the following URL:

  http://java.sun.com/

- CSCea69632

  When run using Netscape version 4.79, all SDM windows display a blank signature in the lower left corner. The text "Signed by:" appears, but no signature text follows.

  Workaround

  None needed. This does not affect the operation of the router.

- CSCea68007

  Due to an IOS caveat, if you configure an Ethernet connection with a dialer-pool command, such as a PPPoE connection, subsequently delete the connection, then configure an ATM connection with PPPoE, and then recreate the Ethernet connection with the **dialer-pool** command, that Ethernet configuration will contain multiple **dialer-pool** statements, and be read-only in SDM.

  Workaround

  Use the CLI to remove all PPPoE and dialer-pool statements from the Ethernet interface configuration. After saving the configuration, save the running configuration to the startup configuration. Then, reload the router and reconfigure the Ethernet connection.

- CSCin46907

  If SDM is using SSH to communicate with the router, it may occasionally display a message box indicating that it can no longer communicate with the router when the user tries to deliver configuration changes. Clicking OK in this message box causes SDM to terminate.

05/2005 - CN
CORREIOS
Fls. Nº 0341
3690

Workaround

Reconfigure the router so that SDM will use Telnet to communicate with it.

To do so using SDM, do the following

- Restart SDM.
- When the SSH Username and Password dialog is displayed, click **Cancel**. SDM will display the Telnet Username and Password dialog.
- Enter a valid username and password in the Telnet dialog and click OK.

Alternatively, you can make this change using the CLI, by doing the following:

- Log on to the router using Telnet, and enter configuration mode.
- Enter the following Cisco IOS commands in config mode:

```
router(config)#line vty 0 15
router(config-line)#transport input telnet
router(config-line)#end
```

- Restart SDM.

With this configuration change, SDM will use Telnet to communicate to the router.

- CSCin48956

When configuring Point-to-Point Protocol over Ethernet (PPPoE) for the Cisco 1711 or 1712 VLAN1 interfaces, SDM does not deliver the **ip tcp adjust-mss** command to the router's configuration.

Workaround

Use the CLI to add the **ip tcp adjust-mss** command to the VLAN1 interface configuration. Telnet to the router and enter the following command in VLAN1 interface configuration mode.

ip tcp adjust-mss 1452

Documentation Updates

The following sections explain how documentation may be inaccurate or incomplete.

REG Nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0342
Doc 3690

Omissions

The following sections explain information that was not included in documentation.

SDM Default Configuration File

SDM includes a default configuration file. The configuration does the following:

- Provides an IP address for your Fast Ethernet interface, enabling an interface to your LAN
- Enables your router's HTTP server, allowing http access from your LAN
- Creates a default username (**sdm**) and password (**sdm**) with privilege level 15
- Enables Telnet access to the router from your LAN

J4,458

Note The default configuration included does not configure any WAN interfaces. To connect to the Internet, you must use SDM to configure a WAN interface.

It is highly recommended that you change the username and password values because they are well known. SDM will help you change those values. Please refer your router's Quick Start Guide for information on how to launch SDM.

Caution If you do not change the username and password values from the default, you will have a security risk because your router will be vulnerable to attacks.

SDM Is Not Supported on SOHO 91, SOHO 96, and SOHO 97 Routers.

The Cisco 831, 836, and 837 Cabling and Setup Quick Start Guides do not state that SDM is not supported on the SOHO 91, SOHO 96, and SOHO 97 routers. The SOHO series of routers do not support SDM.

Modifying the Default Configuration File in Cisco 3620 and 3640 Routers

The instructions provided in the Cisco 3620 and 3640 Modular Access Routers Quick Start Guide for Starting SDM might not work.

The initial communication between a browser running on a PC and SDM is controlled by the default configuration file for the router. On most supported routers, SDM uses a fixed Fast Ethernet port at address `0`, FastEthernet 0/0 or FastEthernet 0. The PC is connected to this interface, and the interface is given an IP address in the default configuration file that SDM recognizes.

For the 3620 and 3640 routers there are no fixed Ethernet ports.

By convention many of these routers ship with a FastEthernet capable network module in Slot 0. SDM assumes this to be the case in its default configuration file. If this is not true for your router, you need to modify the default configuration file to enable and provide an IP address for an Ethernet interface before SDM can communicate with the router.

Perform the following steps to enable SDM to communicate with the browser:

Step 1 Log on to the router using the Console port, using the user name sdm, and password sdm.

Step 2 Enter Enable mode using the password sdm.

Step 3 Provide the IP address 10.10.10.1 and the subnet mask 255.255.255.0 for the interface you will connect the PC to, and enter the no shutdown command to enable the interface.

Step 4 Save the configuration.

Step 5 Connect a PC running a supported browser to the interface you configured.

Step 6 Enter the IP address 10.10.10.1 in the browser to start SDM.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls--Nº 0343
Doc. 3690

14.457
3

Related Documentation

This section lists other documents with information on SDM.

Platform-Specific Documents

Refer to the Quick Start Guide for your router , available on www.cisco.com, to learn how to start SDM for the first time.

Software Documents

These documents are available on www.cisco.com/go/sdm

- Cisco Security Device Manager (SDM) 1.0 Frequently Asked Questions.
- Downloading and Installing Cisco Security Device Manager (SDM) Version 1.0
- Switching Between Cisco Security Device Manager (SDM) and Cisco Router Web Setup Tool (CRWS) on Cisco 83X Series Routers

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0344
Doc 3690

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support

RDS nº 03/2005 - CN
CPMI - CORREIOS
0345
Fls Nº
3690
Doc.

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

CPMI - CORREIOS
Fls Nº 0346
Doc: 3690

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

0347
3690

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

0348
Fls. Nº
3690
Doc.

14.452

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0349
3690
Doc.

14.451
J

Roteador Tipo 1 doc 8

EDS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0350
Doc. 3690

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 and IP Routing Command Reference*. 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 and IP Routing Configuration Guide*. For multiprotocol BGP command descriptions, refer to the "Multiprotocol BGP Extensions for IP Multicast Commands" chapter of the *Cisco IOS IP and IP Routing Command Reference*.

The Border Gateway Protocol, 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 document.

Cisco's 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 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.

03/2005 - CN
CORREIOS
Fls. Nº
0351
Doc. 3690

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 OSPF, Enhanced IGRP, and ISIS-IP, and 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 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 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** 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 Multi Exit Discriminator (MED) metric attribute.

   This comparison is only done if the neighboring autonomous system is the same for all routes considered, unless **bgp always-compare-med** is enabled.

   Note The most recent 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** command.
9. Prefer the external (EBGP) path over the internal (IBGP) path.

   All confederation paths are considered internal paths.

0352
3690

10. Prefer the route that can be reached through the closest IGP neighbor (the lowest IGP metric).

    This means 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.
    - **maximum-paths** 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 AS, 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 AS, instead of picking one best path, 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. The first two basic tasks are required to configure BGP; the remaining basic and advanced tasks are optional.

Basic BGP configuration tasks are discussed in the following sections:

- 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 AS 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)

0353
CPMI
3690 P1C-233
Doc

- Configuring the BGP Version (Optional)
- Configuring the Multi Exit Discriminator Metric (Optional)
- Configuring the Multi Exit Discriminator Metric (Optional)

Advanced BGP Configuration Task List

Advanced, optional BGP configuration tasks are discussed 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 Sub-AS 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."

0354
Fls. Nº
3690

Configuring Basic BGP Features

The tasks in this section are for configuring basic BGP features.

Enabling BGP Routing

To enable BGP routing, establish a BGP routing process by using the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# router bgp autonomous-system` `Router(config-router)#`	Enables a BGP routing process, which places you 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 enter 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 is in contrast to Interior Gateway Protocols (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 router's resources, 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** command to achieve the same result.

Configuring BGP Neighbors

Like other Exterior Gateway Protocols (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, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} remote-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.

ROS nº 03/2005 - CPI
0355
Fls. Nº
3690
Doc
P1C-235

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 7 lists the advantages and disadvantages hard reset and soft reset.

Table 7 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 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** 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.

14.445
RQS nº 03/2005
CPMI
Fls. Nº 0356
Doc 3690

A soft reset updates the routing table for inbound and outbound routing updates. Cisco IOS software releases 12.1 and later 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.

- 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** command, described in "Configuring BGP Soft Reset Using Stored Routing Policy Information." This 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, beginning in EXEC mode:

Command	Purpose
`Router# show ip bgp neighbors ip-address`	Shows 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 **clear ip bgp** command beginning in EXEC mode:

Command	Purpose
`Router# clear ip bgp {* | address | peer-group-name} soft in`	Performs a dynamic soft reset on the connection specified in the command. The *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.

ECOS nº 03/2005 - CN
CPMI CORREIOS
0357
3690

Resetting a Router Using BGP Outbound Soft Reset

Outbound soft resets do not require any preconfiguration. Using the keyword **soft** specifies that a soft reset be performed. To perform an outbound soft reset, use the **clear ip bgp** command, beginning in EXEC mode:

Command	Purpose
`Router# clear ip bgp {* | address | peer-group-name} soft out`	Performs a soft reset on the connection specified in the command. The *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** command. The **clear ip bgp** command initiates the soft reset, which generates a new set of inbound routing table updates using the stored information.

Keep in mind 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. Our 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 {* | 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 Example" section at the end of this chapter for an example of BGP path filtering by neighbor.

0358
3690

Verifying BGP Soft Reset

You can verify whether a soft reset is successful by checking information about the routing table and about BGP neighbors.

Step 1 Enter the **show ip bgp** 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** 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, it is very important that your autonomous system be 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 from happening, BGP must wait until the IGP has propagated routing information across your autonomous system. This causes BGP to be *synchronized* with the IGP. Synchronization is enabled by default.

In some cases, you do not need synchronization. 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 **no synchronization** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# no synchronization`	Disables synchronization between BGP and an IGP.

0360
3690

See the "BGP Path Filtering by Neighbor Example" 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. Just 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. This 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 AS-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 our 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 AS Path Comparison

RFC 1771, the IETF document defining BGP, does not include as-path as part of the "tie-breaker" decision algorithm. By default, Cisco IOS software considers the as-path as a part of the decision algorithm. This enhancement makes it possible to modify the decision algorithm, bringing the router's behavior in selecting a path more in line with the IETF specification.

To prevent the router from considering the as-path length when selecting a route, use the **bgp bestpath as-path ignore** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# bgp bestpath as-path ignore`	Configures the router to ignore as-path length in selecting a route.

0361
3690

Configuring BGP Route Filtering by Neighbor

You can filter BGP advertisements in two ways:

- Use AS-path filters, as with the **ip as-path access-list** global configuration command and the **neighbor filter-list** command
- Use access or prefix lists, as with the **neighbor distribute-list** 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. To do this, 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 **neighbor distribute-list** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} distribute-list {access-list-number | name} {in | out}`	Filters BGP routing updates to/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.

ROS
OPML
File N° 0362
3690
Doc

Configuring BGP Filtering Using Prefix Lists

Prefix lists can be used as an alternative to access lists in many BGP route filtering commands. "How the System Filters Traffic by Prefix List" describes the way prefix list filtering works. The advantages of using prefix lists are:

- 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

  The command-line interface for using access lists to filter BGP updates is difficult to understand and use, since 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 does not need to 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 argument *seq* in the **ip prefix-list** 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 *seq-value* argument of the **ip prefix-list** command.

Regardless of whether the default sequence numbers are used in configuring a prefix list, a sequence number does not need to 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 **ip prefix-list** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# ip prefix-list` *list-name* `[seq` *seq-value*`] deny | permit` *network/len* `[ge` *ge-value*`] [le` *le-value*`]`	Creates a prefix list with the name specified for *list-name*.

0363
P1C-243

14.437

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 **no ip prefix-list** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list list-name [seq seq-value] deny | permit network/len [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 **ip prefix-list** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# ip prefix-list list-name seq seq-value deny | permit network/len [ge ge-value] [le le-value]`	Creates an entry in a prefix list and assigns a sequence number to the entry.

The optional keywords **ge** and **le** can be used to specify the range of the prefix length to be matched for prefixes that are more specific than *network/len*. 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* and/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, you would use:

```
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 command **no ip prefix-list sequence-number**. 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 have 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.

Ex № 0364
3690
Doc

To disable the automatic generation of sequence numbers, use the **no ip prefix-list sequence-number** command, beginning 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 reenable automatic generation of the sequence numbers of prefix list entries, use the **ip prefix-list sequence number** command, beginning 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 *seq-value* argument of the ip **prefix-list** command.

Regardless of whether the default sequence numbers are used in configuring a prefix list, a sequence number does not need to be specified when de-configuring 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 **no ip prefix-list** command, beginning 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 **no ip prefix-list seq** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list seq seq-value`	Deletes an entry in a prefix list.

Note The sequence number of an entry does not need to be specified when you delete the entry.

Showing 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, beginning in EXEC mode:

Command	Purpose
Router# **show ip prefix-list** [**detail** | **summary**]	Displays information about all prefix lists.
Router# **show ip prefix-list** [**detail** | **summary**] *name*	Displays a table showing the entries in a prefix list.
Router# **show ip prefix-list** *name* [**network/len**]	Displays the policy associated with the node.
Router# **show ip prefix-list** *name* [**seq** *seq-num*]	Displays the prefix list entry with a given sequence number.
Router# **show ip prefix-list** *name* [**network/len**] **longer**	Displays all entries of a prefix list that are more specific than the given network and length.
Router# **show ip prefix-list** *name* [**network/len**] **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 **clear ip prefix-list** command, beginning in EXEC mode:

Command	Purpose
Router# **clear ip prefix-list** *name* [**network/len**]	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 do this, 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 *Dial Services Command Reference* 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-regular-expression*	Defines a BGP-related access list.
Step 2	Router# **router bgp** *autonomous-system*	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 Example" section at the end of this chapter for an example of BGP path filtering by neighbor.

0366
3690

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. This 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 **neighbor next-hop-self** command, beginning 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 is useful in a nonmeshed environment, since you know that a path exists from the present router to that address. In a fully meshed environment, this is not useful, since 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** command.

To configure the neighbor peering address to be used for the next hop address, use the **set ip next-hop** command, beginning 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.

0367
3690

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 **neighbor version** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} version value`	Specifies the BGP version to use when communicating with a neighbor.

Configuring the Multi Exit Discriminator Metric

BGP uses the Multi Exit Discriminator (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.) You can set the MED of the redistributed routes by performing the following task. All the routes without a MED will also be set to this value. Use the **default-metric** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# default-metric number`	Sets a multi exit discriminator.

Alternatively, you can set the MED using the **route-map** 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.

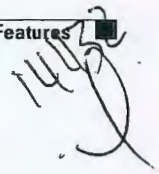
Using Route Maps to Modify Updates

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** command, community based matching requires the **community-list** command and network-based matching requires the **ip access-list** command. Use the **neighbor route-map** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} route-map route-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. If you want the EBGP session to be reset as soon as an interface goes down, use the **bgp fast-external-fallover** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# bgp fast-external-fallover`	Automatically resets EBGP sessions.

Configuring Aggregate Addresses

Classless interdomain routing (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 conditional aggregation feature described in the following task table. An aggregate address will be added to the BGP table if there is at least one more specific entry in the BGP table.

To create an aggregate address in the routing table, use one or more of the following commands, beginning 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 **no auto-summary** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# no auto-summary`	Disables automatic network summarization.

3689
PIC-249

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 AS_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 a BGP speaker's configuration 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 **ip community-list** command, beginning 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** 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. You can specify that the COMMUNITIES attribute be sent to the neighbor at an IP address by using the **neighbor send-community** command, beginning in router configuration mode:

0370
Doc 3690

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 **set comm-list delete** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# set comm-list list-num 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 two bytes long in the **show ip bgp community** command output, as well as 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 AS 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 **ip bgp-community new-format** command, beginning in global configuration mode:

Command	Purpose
`Router(config)# ip bgp-community new-format`	Displays and parses BGP communities in the format AA:NN.

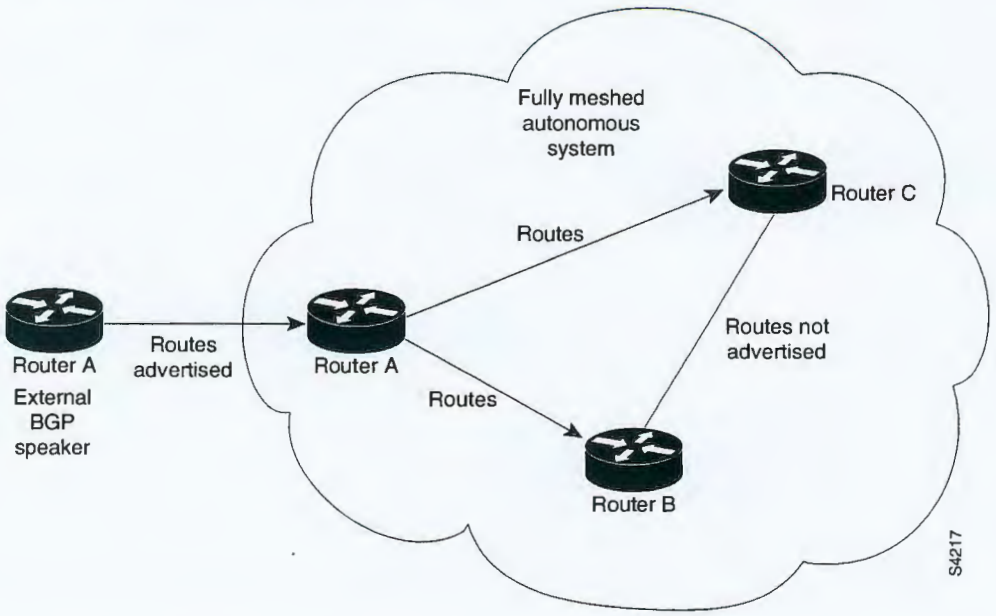
Configuring BGP Conditional Advertisement

The 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.

This feature 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.

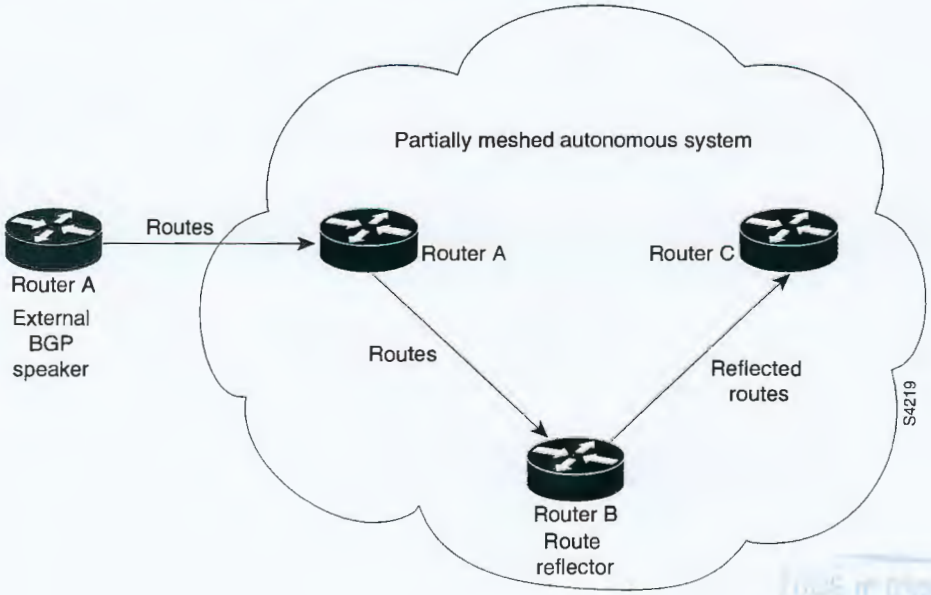
0371
3690

Figure 39 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 internal BGP peer is configured to be a route reflector responsible for passing IBGP learned routes to a set of IBGP neighbors. In Figure 40, 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 40 Simple BGP Model with a Route Reflector

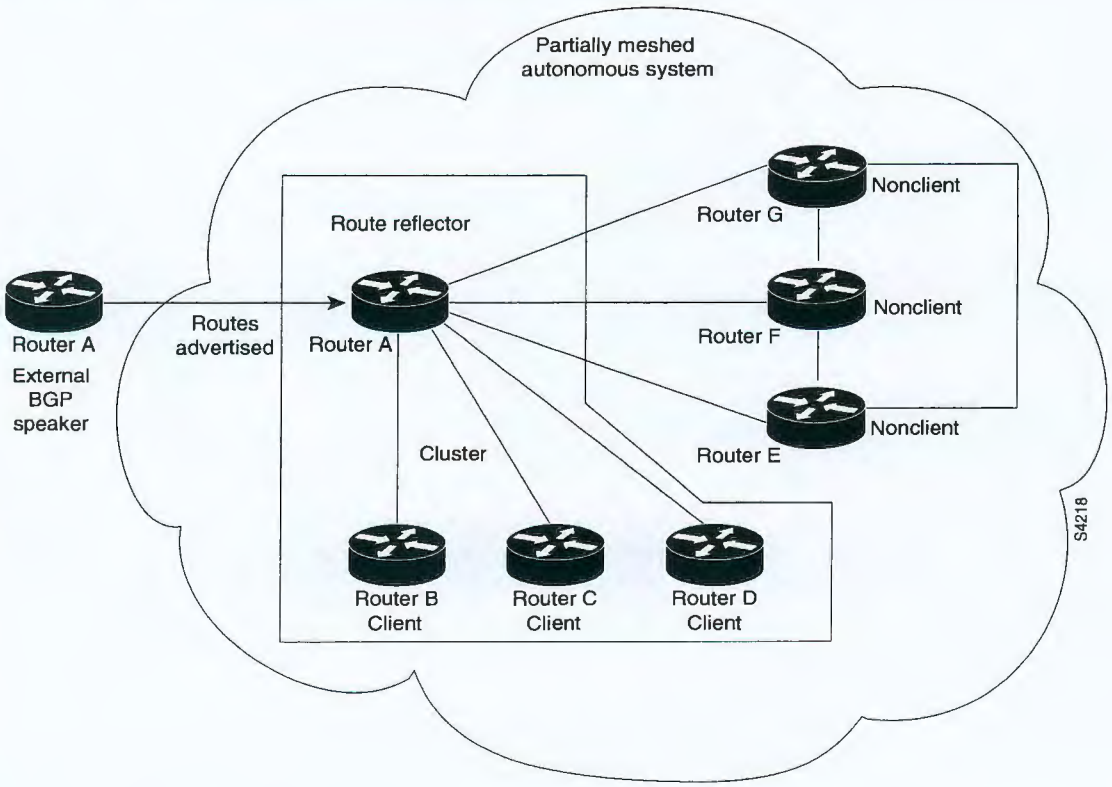


0372
3690

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 41 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.

Figure 41 More Complex BGP Route Reflector Model



When the route reflector receives an advertised route, depending on the neighbor, it does the following:

- 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 **neighbor route-reflector-client** command, beginning 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. This allows easy, 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 **bgp cluster-id** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# bgp cluster-id cluster-id`	Configures the cluster ID.

Use the **show ip bgp** 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 does not need to reflect routes to clients. To disable client-to-client route reflection, use the **no bgp client-to-client reflection** command, beginning 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, it is possible for routing information to loop. The route reflector model has the following mechanisms to avoid routing loops:

- Originator-ID is an optional, nontransitive BGP attribute. This 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, it creates a new one. 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.
- Using **set** clauses in outbound route maps modifies attributes, possibly creating routing loops. To avoid this, **set** clauses of outbound route maps are ignored for routes reflected to IBGP peers.

ROS nº 0374
Fls. Nº
3690

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** command.

Creating the Peer Group

To create a BGP peer group, use the **neighbor peer-group** command, beginning 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: remote-as (if configured), version, update-source, out-route-map, out-filter-list, out-dist-list, minimum-advertisement-interval, and next-hop-self. 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 any of these commands, beginning in router configuration mode.

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} remote-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`	Allows internal BGP sessions to use any operational interface for TCP connections.

RCS
CPM
File No. 0375 3690
Doc

Command	Purpose
`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 multi-hop peer's address 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 | name} {in | out}`	Filters BGP routing updates to/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.
`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, the members can be configured with the **neighbor remote-as** command. This 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** 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 multihop peer's address 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 router A's routes to router C.

0376
3690

1442

For internal BGP, you might want to allow your BGP connections to stay up regardless of which interface is used to reach a neighbor. To do this, 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

Finally, to configure a BGP neighbor to be a member of that BGP peer group, use the **neighbor peer-group** command, beginning 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 **neighbor shutdown** command, beginning 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** command, use the **no neighbor shutdown** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# no neighbor {ip-address | peer-group-name} shutdown`	Enables a BGP neighbor or peer group.

REG nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0377
Doc 3690

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 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 **table-map** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# table-map route-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 internal BGP 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 **distance bgp** command beginning 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.

005 - CN
CORREIOS
0378
3690

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 holdtime 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 **timers bgp** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# timers bgp keepalive holdtime`	Adjusts BGP timers for all neighbors.

To adjust BTP keepalive and holdtime timers for a specific neighbor, use the **neighbor timers** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor [ip-address | peer group-name] timers keepalive holdtime`	Sets the keepalive and holdtime 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** 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 **bgp default local-preference** command, beginning 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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0379
Doc. 3690

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 **default-information originate** command, beginning 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 **bgp bestpath med missing-as-worst** command, beginning 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 **bgp always-compare-med** command, beginning 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 Sub-AS Paths

To configure the router to consider the MED value in choosing a path, use the **bgp bestpath med confed** command, beginning 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 sub-ASs within a confederation.

CPMI - CORREIOS
Fls Nº 0380
3690

The comparison between MEDs is only made if there are no external ASes in the path (an external AS is an AS that is not within the confederation). If there is an external AS in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

For e and we are comparing 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 **bgp bestpath med confed** is enabled. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external AS 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 sub-AS within a confederation, use the **bgp deterministic med** command, beginning 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 **bgp always-compare-med** is enabled, all paths are fully comparable, including those from other ASes in the confederation, even if **bgp deterministic med** 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: AS 1, AS 2, and AS 3. Suppose the route to network A in AS 1 flaps (it becomes unavailable). Under circumstances without route dampening, AS 1's EBGP neighbor to AS 2 sends a Withdraw message to AS 2. The border router in AS 2, in turn, propagates the Withdraw to AS 3. When the route to network A reappears, AS 1 sends an Advertisement to AS 2, which sends it to AS 3. If the route to network A repeatedly becomes unavailable, then available, many Withdrawals and Advertisements 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, there is no penalty applied in this instance, even if route flap dampening is enabled.

03/2005 - CN
CORREIOS
0381
3690

Minimizing Flapping

The route dampening feature minimizes the flapping problem as follows. Suppose again that the route to network A flaps. The router in AS 2 (where route dampening is enabled) assigns network A a penalty of 1000 and moves it to "history" state. The router in AS 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 AS 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 4 times the half-life.

The routes external to an AS learned via IBGP are not dampened. This policy prevent the IBGP peers from having a higher penalty for routes external to the AS.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0382
3690

Enabling Route Dampening

To enable BGP route dampening, use the **bgp dampening** command, beginning in global configuration mode:

Command	Purpose
`Router(config)# bgp dampening`	Enables BGP route dampening.

To change the default values of various dampening factors, use the **bgp dampening** command, beginning in global configuration mode:

Command	Purpose
`Router(config)# bgp dampening` *half-life reuse suppress max-suppress* `[route-map` *map*`]`	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, beginning in EXEC mode:

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` *list*	Displays BGP flap statistics for all paths that pass the filter.
`Router# show ip bgp flap-statistics` *address mask*	Displays BGP flap statistics for a single entry.
`Router# show ip bgp flap-statistics` *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, beginning in EXEC mode:

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` *address mask*	Clears BGP flap statistics for a single entry.
`Router# clear ip bgp` *address* `flap-statistics`	Clears BGP flap statistics for all paths from a neighbor.

0383
3690

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 **show ip bgp dampened-paths** command, beginning 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 **clear ip bgp dampening** command, beginning in EXEC mode:

Command	Purpose
Router# **clear ip bgp dampening** [*address mask*]	Clears route dampening information and unsuppress 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.

The following table lists the tasks associated with clearing caches, tables, and databases for BGP. Use these commands, beginning in EXEC mode:

Command	Purpose
Router# **clear ip bgp** *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.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0384
Doc. 3690

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 your device's packets are taking through the network.

To display various routing statistics, use the following commands, beginning in EXEC mode:

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.
R r# **show ip bgp community** *community-number* **exact**]	Displays routes that belong to the specified communities.
uter# **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** *regular-expression*	Displays the routes that have an AS 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** [*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** *regular-expression* | **dampened-routes**]	Displays routes learned from a particular BGP neighbor.
Router# **show ip bgp paths**	Displays all BGP paths in the database.
R r# **show ip bgp peer-group** [*tag*] [**summary**]	Displays information about BGP peer groups.
uter# **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 **bgp log-neighbor changes** command, beginning 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

0385
3690

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 Example
- BGP Path Filtering by Neighbor Example
- BGP Aggregate Route Examples
- BGP Community with Route Maps Examples
- BGP Conditional Advertisement Configuration Examples
- BGP Confederation Example
- BGP Peer Group Examples
- TCP MD5 Authentication for BGP Example

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, route map freddy marks all paths originating from autonomous system 690 with a Multi Exit Discriminator (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
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0386
3690

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 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 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 called 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
```

n° 03/2005 - CN
CORREIOS
0387
Fls N°
3690

```
!
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 do prefix-based matching and set various parameters of the update. Inbound prefix matching is available in addition to as-path and community-list matching. The following example shows how the **set local preference** 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 B, and B peers with C. B sends traffic over the routes of router A to router C, but wants to make sure that all traffic from C to A goes through B, rather than directly from C to A over the shared LAN. This configuration can be useful for traffic accounting purposes or to satisfy the peering agreement between C and B. You can achieve this configuration by using the **set ip next-hop** 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

```
router bgp 100
 neighbor 1.1.1.2 remote-as 200
```

Router B

```
router bgp 200
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.3 remote-as 300
```

Router C

```
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
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0388
Doc 3690

Example two applies an outbound route map on the BGP session of router B with router C.

Router A

```
router bgp 100
 neighbor 1.1.1.2 remote-as 200
```

Router B

```
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

```
router bgp 300
 neighbor 1.1.1.2 remote-as 200
```

BGP Neighbor Configuration Examples

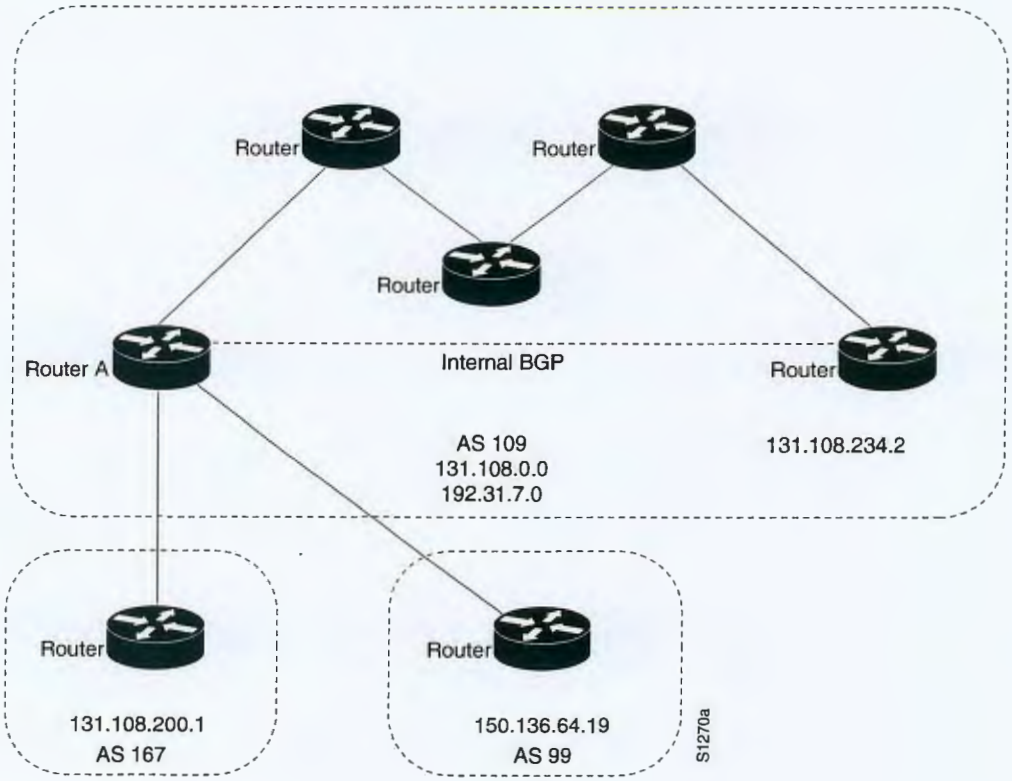
The following example shows how BGP neighbors on an autonomous system are configured to share information. In the example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous 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** command specifies an internal neighbor (with the same autonomous system number) at address 131.108.234.2; and the third **neighbor** 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 42, Router A is being configured. The internal BGP 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.

ROS nº 03/2005 - CN
GPMI - CORREIOS
Fls. Nº 0389
3690

Figure 42 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
!
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
0390
Fls Nº
3690

The following example configuration shows how to conditionally originate a default route(0.0.0.0/0) in RIP when there exists a prefix 10.1.1.0/24 in the routing table:

```
ip prefix-list cond permit 10.1.1.0/24
!
route-map default-condition permit 10
match ip address prefix-list cond
!
router rip
default-information originate route-map default-condition !
```

The following example shows how to configure BGP to accept routing updates from 192.1.1.1 only, besides filtering on the prefix length:

```
router bgp
distribute-list prefix max24 gateway allowlist in
!
ip prefix-list allowlist seq 5 permit 192.1.1.1/32
!
```

The following example shows how to direct the BGP process to filter incoming updates to the prefix using *name1*, and match the gateway (next-hop) of the prefix being updated to the prefix list *name2*, on the interface ethernet 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 prefix length up to 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

The following example shows how to configure BGP to deny routes with 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 prefix length greater than 8 and less than 24 in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to configure BGP to deny routes with 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, since any route in the Class A network 10.0.0.0/8 is denied if its mask is less than or equal to 32 bits:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to configure BGP to deny routes with a mask greater than 25 in 204.70.1/24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

The following example shows how to configure BGP to permit all routes:

```
ip prefix-list abc permit 0.0.0.0/0 le 32
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0391
3690
Doc.

Added or Deleted Prefix List Entries Examples

You can add or delete individual entries in a prefix list. For example, 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 172.16.0.0/8
ip prefix-list abc permit 192.168.0.0/15
```

The following example shows how to delete an entry from the prefix list so that 192.168.0.0 is not permitted, and add a a new entry that permits 10.0.0.0/8:

```
no ip prefix-list abc permit 192.168.0.0/15
ip prefix-list abc permit 10.0.0.0/8
```

The new configuration is:

```
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 172.16.0.0/8
ip prefix-list abc permit 10.0.0.0/8
```

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** command used to initiate a dynamic soft reconfiguration in the BGP peer 131.108.1.1. This command requires that the peer supports the route refresh capability.

```
Router# 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.

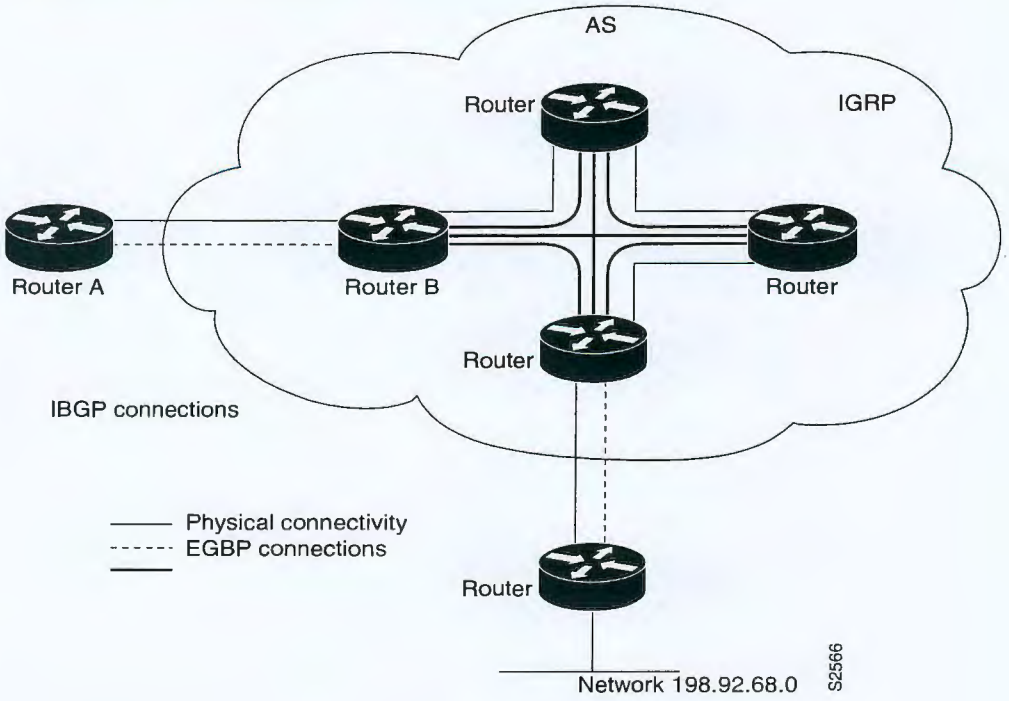
```
clear ip bgp 131.108.1.1 soft in
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0392
Doc. 3690

BGP Synchronization Example

The example shown in Figure 43 shows how to use the **no synchronization** 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 internal BGP mesh.

Figure 43 BGP Synchronization Configuration



BGP Path Filtering by Neighbor Example

The following example shows BGP path filtering by neighbor. Only the routes that pass as-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 .*
```

- CN
CPMI - CORREIOS
0393
Fls Nº
3690

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 conditional aggregate routing feature.

In the following example, the **redistribute static** command is used to redistribute aggregate route 193.*.*.*:

```
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 there is at least one specific route that 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** 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.*.*.*, 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 "BGP Confederation Example" in this chapter.

The first example shows how the route map 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
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº
0394
Doc. 3690

The second example shows how the route map *set-community* is applied to the outbound updates to neighbor 171.69.232.90. All the routes that originate from AS 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. This includes 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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0395
Fls. Nº
Doc 3690

The next example shows how the route map *set-community* is applied to the outbound updates to the 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 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 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 sub-autonomous 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 sub-autonomous 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 sub-autonomous 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* arguments and *map2-name,* 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.

ROSINI 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0396
3690
Doc

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 Example

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** command).

In a BGP speaker in autonomous system 6001, the **bgp confederation peers** 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. 200.200.200.200.200 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
```

RQS nº 03/2005 - CN
CRMI - CORREIOS
Fls. Nº 0397
Doc. 3690

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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0398
Fls Nº
Doc 3690

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.

ECT 03/2005 - CN
CORREIOS
0399
3690

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
`.outer(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.

ECT 03/2005 - CN
CPMI - CORREIOS
0400
Fls.
3690
Doc.

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
```

- CN
- CORREIOS
0401
3690

Roteador Tipo 1 doc 10

RQS nº 03/2005 - CPMI - CORREIOS
Fls Nº 0402
3690

Configuring OSPF

This chapter describes how to configure OSPF. For a complete description of the OSPF commands in this chapter, refer to the "OSPF Commands" chapter of the *Network Protocols Command Reference, Part 1*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Open shortest path first (OSPF) is an IGP developed by the OSPF working group of the Internet Engineering Task Force (IETF). Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending/receiving packets.

We support RFC 1253, Open Shortest Path First (OSPF) MIB, August 1991. The OSPF MIB defines an IP routing protocol that provides management information related to OSPF and is supported by Cisco routers.

For protocol-independent features that include OSPF, see the chapter "Configuring IP Routing Protocol-Independent Features" in this document.

Cisco's OSPF Implementation

Cisco's implementation conforms to the OSPF Version 2 specifications detailed in the Internet RFC 1583. The list that follows outlines key features supported in Cisco's OSPF implementation:

- Stub areas—Definition of stub areas is supported.
- Route redistribution—Routes learned via any IP routing protocol can be redistributed into any other IP routing protocol. At the intradomain level, this means that OSPF can import routes learned via IGRP, RIP, and IS-IS. OSPF routes can also be exported into IGRP, RIP, and IS-IS. At the interdomain level, OSPF can import routes learned via EGP and BGP. OSPF routes can be exported into EGP and BGP.
- Authentication—Plain text and MD5 authentication among neighboring routers within an area is supported.
- Routing interface parameters—Configurable parameters supported include interface output cost, retransmission interval, interface transmit delay, router priority, router "dead" and hello intervals, and authentication key.
- Virtual links—Virtual links are supported.
- NSSA areas—RFC 1587.
- OSPF over demand circuit—RFC 1793.

ROS nº 03/2005 6N
CPMI - CORREIOS
Fls Nº 6403
Doc: 3690

OSPF Configuration Task List

OSPF typically requires coordination among many internal routers, *area border routers* (routers connected to multiple areas), and autonomous system boundary routers. At a minimum, OSPF-based routers or access servers can be configured with all default parameter values, no authentication, and interfaces assigned to areas. If you intend to customize your environment, you must ensure coordinated configurations of all routers.

To configure OSPF, complete the tasks in the following sections. Enabling OSPF is mandatory; the other tasks are optional, but might be required for your application.

- Enable OSPF
- Configure OSPF Interface Parameters
- Configure OSPF over Different Physical Networks
- Configure OSPF Area Parameters
- Configure OSPF Not So Stubby Area (NSSA)
- Configure Route Summarization between OSPF Areas
- Configure Route Summarization when Redistributing Routes into OSPF
- Create Virtual Links
- Generate a Default Route
- Configure Lookup of DNS Names
- Force the Router ID Choice with a Loopback Interface
- Control Default Metrics
- Change the OSPF Administrative Distances
- Configure OSPF on Simplex Ethernet Interfaces
- Configure Route Calculation Timers
- Configure OSPF over On Demand Circuits
- Log Neighbors Going Up or Down
- Change the LSA Group Pacing
- Block OSPF LSA Flooding
- Ignore MOSPF LSA Packets
- Monitor and Maintain OSPF

In addition, you can specify route redistribution; see the task "Redistribute Routing Information" in the chapter "Configuring IP Routing Protocol-Independent Features" for information on how to configure route redistribution.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0404
Doc. 3690

Enable OSPF

As with other routing protocols, enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses. Use the following commands, starting in global configuration mode:

Step	Command	Purpose
1	**router ospf** *process-id*	Enable OSPF routing, which places you in router configuration mode.
2	**network** *address wildcard-mask* **area** *area-id*	Define an interface on which OSPF runs and define the area ID for that interface.

Configure OSPF Interface Parameters

Our OSPF implementation allows you to alter certain interface-specific OSPF parameters, as needed. You are not required to alter any of these parameters, but some interface parameters must be consistent across all routers in an attached network. Those parameters are controlled by the **ip ospf hello-interval**, **ip ospf dead-interval**, and **ip ospf authentication-key** commands. Therefore, be sure that if you do configure any of these parameters, the configurations for all routers on your network have compatible values.

In interface configuration mode, use any of the following commands to specify interface parameters as needed for your network:

Command	Purpose
ip ospf cost *cost*	Explicitly specify the cost of sending a packet on an OSPF interface.
ip ospf retransmit-interval *seconds*	Specify the number of seconds between link state advertisement retransmissions for adjacencies belonging to an OSPF interface.
ip ospf transmit-delay *seconds*	Set the estimated number of seconds it takes to transmit a link state update packet on an OSPF interface.
ip ospf priority *number*	Set priority to help determine the OSPF designated router for a network.
ip ospf hello-interval *seconds*	Specify the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.
ip ospf dead-interval *seconds*	Set the number of seconds that a device's hello packets must not have been seen before its neighbors declare the OSPF router down.
ip ospf authentication-key *key*	Assign a password to be used by neighboring OSPF routers on a network segment that is using OSPF's simple password authentication.
ip ospf message-digest-key *keyid* **md5** *key*	Enable OSPF MD5 authentication.
ip ospf authentication [message-digest | null]	Specifies the authentication type for an interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0405
Fls Nº
3690
Doc.

Configure OSPF over Different Physical Networks

OSPF classifies different media into the following three types of networks by default:

- Broadcast networks (Ethernet, Token Ring, FDDI)
- Nonbroadcast multiaccess networks (SMDS, Frame Relay, X.25)
- Point-to-point networks (HDLC, PPP)

You can configure your network as either a broadcast or a nonbroadcast multiaccess network.

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. See the **x25 map** and **frame-relay map** command descriptions in the *Wide-Area Networking Command Reference* for more detail.

Configure Your OSPF Network Type

You have the choice of configuring your OSPF network type as either broadcast or nonbroadcast multiaccess, regardless of the default media type. Using this feature, you can configure broadcast networks as nonbroadcast multiaccess networks when, for example, you have routers in your network that do not support multicast addressing. You also can configure nonbroadcast multiaccess networks (such as X.25, Frame Relay, and SMDS) as broadcast networks. This feature saves you from having to configure neighbors, as described in the section "Configure OSPF for Nonbroadcast Networks."

Configuring nonbroadcast, multiaccess networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed network. This is not true for some cases, for example, because of cost constraints, or when you have only a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers not directly connected will go through the router that has virtual circuits to both routers. Note that it is not necessary to configure neighbors when using this feature.

An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes. An OSPF point-to-multipoint network has the following benefits compared to nonbroadcast multiaccess and point-to-point networks:

- Point-to-multipoint is easier to configure because it requires no configuration of neighbor commands, it consumes only one IP subnet, and it requires no designated router election.
- It costs less because it does not require a fully meshed topology.
- It is more reliable because it maintains connectivity in the event of virtual circuit failure.

To configure your OSPF network type, use the following command in interface configuration mode:

Command	Purpose
ip ospf network {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] }}	Configure the OSPF network type for a specified interface.

See the "OSPF Point-to-Multipoint Example" section at the end of this chapter for an example of an OSPF point-to-multipoint network.

ECT/ECP - CORREIOS
Fls Nº 0406
3690

Configure Point-to-Multipoint, Broadcast Networks

On point-to-multipoint, broadcast networks, there is no need to specify neighbors. However, you can specify neighbors with the **neighbor** command, in which case you should specify a cost to that neighbor.

Before this feature, some OSPF point-to-multipoint protocol traffic was treated as multicast traffic. Therefore, the **neighbor** command was not needed for point-to-multipoint interfaces because multicast took care of the traffic. Hellos, updates and acknowledgments were sent using multicast. In particular, multicast hellos discovered all neighbors dynamically.

On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumed the cost to each neighbor was equal. The cost was configured with the **ip ospf cost** command. In reality, the bandwidth to each neighbor is different, so the cost should be different. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

To treat an interface as point-to-multipoint broadcast and assign a cost to each neighbor, use the following commands beginning in interface configuration mode:

Step	Command	Purpose
1	**ip ospf network point-to-multipoint**	Configure an interface as point-to-multipoint for broadcast media.
2	**exit**	Enter global configuration mode.
3	**router ospf** *process-id*	Configure an OSPF routing process and enter router configuration mode.
4	**neighbor** *ip-address* **cost** *number*	Specify a neighbor and assign a cost to the neighbor.
5		Repeat Step 4 for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the **ip ospf cost** command.

Configure OSPF for Nonbroadcast Networks

Because there might be many routers attached to an OSPF network, a *designated router* is selected for the network. It is necessary to use special configuration parameters in the designated router selection if broadcast capability is not configured.

These parameters need only be configured in those devices that are themselves eligible to become the designated router or backup designated router (in other words, routers with a nonzero router priority value).

To configure routers that interconnect to nonbroadcast networks, use the following command in router configuration mode:

Command	Purpose
neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Configure a router interconnecting to nonbroadcast networks.

You can specify the following neighbor parameters, as required:

- Priority for a neighboring router
- Nonbroadcast poll interval
- Interface through which the neighbor is reachable

On point-to-multipoint, nonbroadcast networks, you now use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Prior to Release 12.0, some customers were using point-to-multipoint on nonbroadcast media (such as classic IP over ATM), so their routers could not dynamically discover their neighbors. This feature allows the **neighbor** command to be used on point-to-multipoint interfaces.

CPMI - CORREIOS
Fls. Nº 3690

On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumed the cost to each neighbor was equal. The cost was configured with the **ip ospf cost** command. In reality, the bandwidth to each neighbor is different, so the cost should be different. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

To treat the interface as point-to-multipoint when the media does not support broadcast, use the following commands beginning in interface configuration mode:

Step	Command	Purpose
1	**ip ospf network point-to-multipoint non-broadcast**	Configure an interface as point-to-multipoint for nonbroadcast media.
2	**exit**	Enter global configuration mode.
3	**router ospf** *process-id*	Configure an OSPF routing process and enter router configuration mode.
4	**neighbor** *ip-address* [**cost** *number*]	Specify an OSPF neighbor and optionally assign a cost to the neighbor.
5		Repeat Step 4 for each neighbor.

Configure OSPF Area Parameters

Our OSPF software allows you to configure several area parameters. These area parameters, shown in the following table, include authentication, defining stub areas, and assigning specific costs to the default summary route. *Authentication* allows password-based protection against unauthorized access to an area.

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the area border router, into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, *default routing* must be used in the stub area. To further reduce the number of link state advertisements sent into a stub area, you can configure **no-summary** on the ABR to prevent it from sending summary link advertisement (link state advertisements Type 3) into the stub area.

In router configuration mode, specify any of the following area parameters as needed for your network:

Command	Purpose
area *area-id* **authentication**	Enable authentication for an OSPF area.
area *area-id* **authentication message-digest**	Enable MD5 authentication for an OSPF area.
area *area-id* **stub** [**no-summary**]	Define an area to be a stub area.
area *area-id* **default-cost** *cost*	Assign a specific cost to the default summary route used for the stub area.

Configure OSPF Not So Stubby Area (NSSA)

NSSA area is similar to OSPF stub area. NSSA does not flood Type 5 external link state advertisements (LSAs) from the core into the area, but it has the ability of importing AS external routes in a limited fashion within the area.

NSSA allows importing of Type 7 AS external routes within NSSA area by redistribution. These Type 7 LSAs are translated into Type 5 LSAs by NSSA ABR which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

0408
ECT - CORREIOS
Fls Nº
3690
Doc.

Use NSSA to simplify administration if you are an Internet service provider (ISP), or a network administrator that must connect a central site using OSPF to a remote site that is using a different routing protocol.

Prior to NSSA, the connection between the corporate site border router and the remote router could not be run as OSPF stub area because routes for the remote site cannot be redistributed into stub area. A simple protocol like RIP is usually run and handle the redistribution. This meant maintaining two routing protocols. With NSSA, you can extend OSPF to cover the remote connection by defining the area between the corporate router and the remote router as an NSSA.

In router configuration mode, use the following command to specify area parameters as needed to configure OSPF NSSA:

Command	Purpose
area *area-id* **nssa [no-redistribution] [default-information-originate]**	Define an area to be NSSA.

In router configuration mode on the ABR, use the following command to control summarization and filtering of Type 7 LSA into Type 5 LSA:

Command	Purpose
summary address *prefix mask* **[not advertise] [tag** *tag*]	(Optional) Control the summarization and filtering during the translation.

Implementation Considerations

Evaluate the following considerations before implementing this feature:

- You can set a Type 7 default route that can be used to reach external destinations. When configured, the router generates a Type 7 default into the NSSA by the NSSA ABR.
- Every router within the same area must agree that the area is NSSA; otherwise, the routers will not be able to communicate with each other.

If possible, avoid using explicit redistribution on NSSA ABR because confusion may result over which packets are being translated by which router.

Configure Route Summarization between OSPF Areas

Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

To specify an address range, use the following command in router configuration mode:

Command	Purpose
area *area-id* **range** *address mask* **[advertise | not-advertise]**	Specify an address range for which a single route will be advertised.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0409
3690
Doc.

Configure Route Summarization when Redistributing Routes into OSPF

When redistributing routes from other protocols into OSPF (as described in the chapter "Configuring IP Routing Protocol-Independent Features"), each route is advertised individually in an external link state advertisement (LSA). However, you can configure the Cisco IOS software to advertise a single route for all the redistributed routes that are covered by a specified network address and mask. Doing so helps decrease the size of the OSPF link state database.

To have the software advertise one summary route for all redistributed routes covered by a network address and mask, use the following command in router configuration mode:

Command	Purpose
summary-address *address mask*	Specify an address and mask that covers redistributed routes, so only one summary route is advertised.

Create Virtual Links

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a *virtual link*. The two end points of a virtual link are Area Border Routers. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR), and the nonbackbone area that the two routers have in common (called the *transit area*). Note that virtual links cannot be configured through stub areas.

To establish a virtual link, use the following command in router configuration mode:

Command	Purpose
area *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [[**authentication-key** *key*] | [**message-digest-key** *keyid* **md5** *key*]]	Establish a virtual link.

To display information about virtual links, use the **show ip ospf virtual-links** EXEC command. To display the router ID of an OSPF router, use the **show ip ospf** EXEC command.

Generate a Default Route

You can force an autonomous system boundary router to generate a default route into an OSPF routing domain. Whenever you specifically configure redistribution of routes into an OSPF routing domain, the router automatically becomes an autonomous system boundary router. However, an autonomous system boundary router does not, by default, generate a *default route* into the OSPF routing domain.

To force the autonomous system boundary router to generate a default route, use the following command in router configuration mode:

Command	Purpose
default-information originate [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]	Force the autonomous system boundary router to generate a default route into the OSPF routing domain.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0410
3690

See the discussion of redistribution of routes in the "Configuring IP Routing Protocol-Independent Features" chapter.

Configure Lookup of DNS Names

You can configure OSPF to look up Domain Naming System (DNS) names for use in all OSPF **show** command displays. This feature makes it easier to identify a router, because it is displayed by name rather than by its router ID or neighbor ID.

To configure DNS name lookup, use the following command in global configuration mode:

Command	Purpose
ip ospf name-lookup	Configure DNS name lookup.

rce the Router ID Choice with a Loopback Interface

OSPF uses the largest IP address configured on the interfaces as its router ID. If the interface associated with this IP address is ever brought down, or if the address is removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces.

If a loopback interface is configured with an IP address, the Cisco IOS software will use this IP address as its router ID, even if other interfaces have larger IP addresses. Since loopback interfaces never go down, greater stability in the routing table is achieved.

OSPF automatically prefers a loopback interface over any other kind, and it chooses the highest IP address among all loopback interfaces. If no loopback interfaces are present, the highest IP address in the router is chosen. You cannot tell OSPF to use any particular interface.

To configure an IP address on a loopback interface, use the following commands, starting in global configuration mode:

Step	Command	Purpose
1	**interface loopback 0**	Create a loopback interface, which places you in interface configuration mode.
2	**ip address** *address mask*	Assign an IP address to this interface.

Control Default Metrics

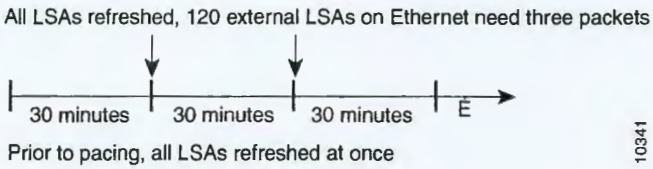
In Cisco IOS Release 10.3 and later, by default, OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link gets a metric of 1562, while a T1 link gets a metric of 64.

The OSPF metric is calculated as *ref-bw* divided by *bandwidth*, with *ref-bw* equal to 10^8 by default, and *bandwidth* determined by the **bandwidth** command. The calculation gives FDDI a metric of 1. If you have multiple links with high bandwidth, you might want to specify a larger number to differentiate the cost on those links. To do so, use the following command in router configuration mode:

Command	Purpose
ospf auto-cost reference-bandwidth *ref-bw*	Differentiate high bandwidth links.

RQS nº 03/2005 - CN
CPMI - CORREIOS
- CN
Fls. Nº 0411
Doc. 3690

Figure 21 OSPF LSAs on a Single Timer without Group Pacing



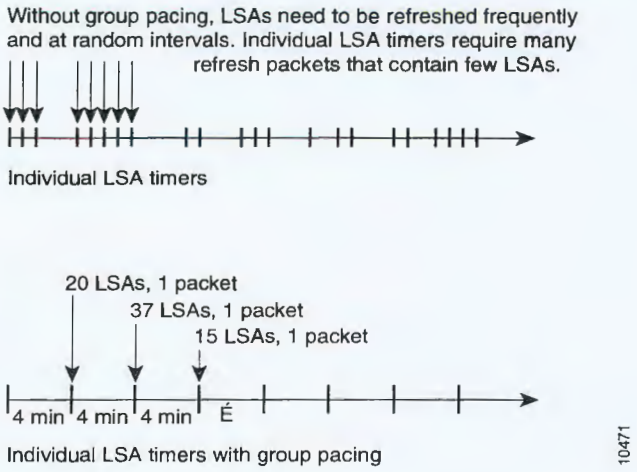
Solution

This problem is solved by each LSA having its own timer. Again using the example of refreshing, each LSA gets refreshed when it is 30 minutes old, independent of other LSAs. So CPU is used only when necessary. However, LSAs being refreshed at frequent, random intervals would require many packets for the few refreshed LSAs the router must send out. That would be inefficient use of bandwidth.

Therefore, the router delays the LSA refresh function for an interval of time instead of performing it when the individual timers are reached. The accumulated LSAs constitute a group, which is then refreshed and sent out in one packet or more. Thus, the refresh packets are paced, as are the checksumming and aging. The pacing interval is configurable; it defaults to 4 minutes, which is randomized to further avoid synchronization.

Figure 22 illustrates the case of refresh packets. The first timeline illustrates individual LSA timers; the second timeline illustrates individual LSA timers with group pacing.

Figure 22 OSPF LSAs on Individual Timers with Group Pacing



RQS nº 03/2005 - CN
CPMI - CORREIOS
0412
Fls Nº
3690
Doc.

The group pacing interval is inversely proportional to the number of LSAs the router is refreshing, checksumming, and aging. For example, if you have approximately 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

The default value of pacing between LSA groups is 240 seconds (4 minutes). The range is 10 seconds to 1800 seconds (half an hour). To change the LSA group pacing interval, use the following command in router configuration mode:

Command	Purpose
timers lsa-group-pacing *seconds*	Change the group pacing of LSAs.

For an example, see the section "LSA Group Pacing Example" at the end of this chapter.

Block OSPF LSA Flooding

By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. Some redundancy is desirable, because it ensures robust flooding. However, too much redundancy can waste bandwidth and might destabilize the network due to excessive link and CPU usage in certain topologies. An example would be a fully meshed topology.

You can block OSPF flooding of LSAs two ways, depending on the type of networks:

- On broadcast, nonbroadcast, and point-to-point networks, you can block flooding over specified OSPF interfaces.
- On point-to-multipoint networks, you can block flooding to a specified neighbor.

On broadcast, nonbroadcast, and point-to-point networks, to prevent flooding of OSPF LSAs, use the following command in interface configuration mode:

Command	Purpose
ospf database-filter all out	Block the flooding of OSPF LSA packets to the interface.

On point-to-multipoint networks, to prevent flooding of OSPF LSAs, use the following command in router configuration mode:

Command	Purpose
neighbor *ip-address* **database-filter all out**	Block the flooding of OSPF LSA packets to the specified neighbor.

For an example of blocking LSA flooding, see the section "Block LSA Flooding Example" at the end of this chapter.

Ignore MOSPF LSA Packets

Cisco routers do not support LSA Type 6 (MOSPF), and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages. To do so, use the following command in router configuration mode:

Command	Purpose
ospf ignore lsa mospf	Prevent the router from generating syslog messages when it receives MOSPF LSA packets.

For an example of suppressing MOSPF LSA packets, see the section "Ignore MOSPF LSA Packets Example" at the end of this chapter.

0413
CPMI CORREIOS
Fls Nº
3690

Monitor and Maintain OSPF

You can display specific statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device's packets are taking through the network.

To display various routing statistics, use the following commands in EXEC mode:

Command	Purpose
show ip ospf [*process-id*]	Display general information about OSPF routing processes.
show ip ospf [*process-id area-id*] **database** **show ip ospf** [*process-id area-id*] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id area-id*] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id area-id*] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id*] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id area-id*] **database** [**database-summary**]	Display lists of information related to the OSPF database.
show ip ospf border-routers	Display the internal OSPF routing table entries to Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).
show ip ospf interface [*interface-name*]	Display OSPF-related interface information.
show ip ospf neighbor [*interface-name*] [*neighbor-id*] **detail**	Display OSPF-neighbor information on a per-interface basis.
show ip ospf request-list [*nbr*] [*intf*] [*intf-nbr*]	Display a list of all LSAs requested by a router.
show ip ospf retransmission-list [*nbr*] [*intf*] [*intf-nbr*]	Display a list of all LSAs waiting to be retransmitted.
show ip ospf virtual-links	Display OSPF-related virtual links information.

OSPF Configuration Examples

The following sections provide OSPF configuration examples:

- OSPF Point-to-Multipoint Example
- OSPF Point-to-Multipoint, Broadcast Example
- OSPF Point-to-Multipoint, Nonbroadcast Example
- Variable-Length Subnet Masks Example
- OSPF Routing and Route Redistribution Examples

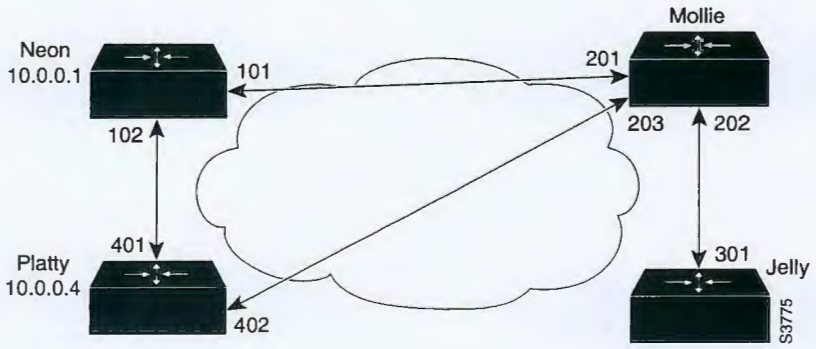
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0414
3690
Doc.

- Route Map Examples
- Changing OSPF Administrative Distance
- OSPF over On-Demand Routing Example
- LSA Group Pacing Example
- Block LSA Flooding Example
- Ignore MOSPF LSA Packets Example

OSPF Point-to-Multipoint Example

In Figure 23, Mollie uses DLCI 201 to communicate with Neon, DLCI 202 to Jelly, and DLCI 203 to Platty. Neon uses DLCI 101 to communicate with Mollie and DLCI 102 to communicate with Platty. Platty communicates with Neon (DLCI 401) and Mollie (DLCI 402). Jelly communicates with Mollie (DLCI 301).

Figure 23 OSPF Point-to-Multipoint Example



Mollie's Configuration

```
hostname mollie
!
interface serial 1
 ip address 10.0.0.2 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 201 broadcast
 frame-relay map ip 10.0.0.3 202 broadcast
 frame-relay map ip 10.0.0.4 203 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0415
Doc. 3690

Neon's Configuration

```
hostname neon
!
interface serial 0
 ip address 10.0.0.1 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.2 101 broadcast
 frame-relay map ip 10.0.0.4 102 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

Platty's Configuration

```
hostname platty
!
interface serial 3
 ip address 10.0.0.4 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 1000000
 frame-relay map ip 10.0.0.1 401 broadcast
 frame-relay map ip 10.0.0.2 402 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

Jelly's Configuration

```
hostname jelly
!
interface serial 2
 ip address 10.0.0.3 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 2000000
 frame-relay map ip 10.0.0.2 301 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

OSPF Point-to-Multipoint, Broadcast Example

The following example illustrates a point-to-multipoint network with broadcast:

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
 ip ospf cost 100
 ip ospf network point-to-multipoint
 frame-relay map ip 10.0.1.3 202 broadcast
 frame-relay map ip 10.0.1.4 203 broadcast
 frame-relay map ip 10.0.1.5 204 broadcast
 frame-relay local-dlci 200
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 neighbor 10.0.1.5 cost 5
 neighbor 10.0.1.4 cost 10
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0416
3690
Doc.

The following example shows the configuration of the neighbor at 10.0.1.3:

```
interface serial 0
 ip address 10.0.1.3 255.255.255.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300 broadcast
 no shut
!
 router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

The output shown for neighbors in the first configuration above looks like this:

```
Router# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
4.1.1.1           1   FULL/  -        00:01:50    10.0.1.5        Serial0
3.1.1.1           1   FULL/  -        00:01:47    10.0.1.4        Serial0
2.1.1.1           1   FULL/  -        00:01:45    10.0.1.3        Serial0
```

The route information in the first configuration above looks like this:

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    1.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.0.1.3/32 [110/100] via 10.0.1.3, 00:39:08, Serial0
C       10.0.1.0/24 is directly connected, Serial0
O       10.0.1.5/32 [110/5] via 10.0.1.5, 00:39:08, Serial0
O       10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0
```

OSPF Point-to-Multipoint, Nonbroadcast Example

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0417
Doc 3690

The following example is the configuration for the router on the other side:

```
interface Serial9/2
 ip address 10.0.1.3 255.255.255.0
 encapsulation frame-relay
 ip ospf network point-to-multipoint non-broadcast
 no ip mroute-cache
 no keepalive
 no fair-queue
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300
 no shut
 !
 router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

The output shown for neighbors in the first configuration above looks like this:

```
Router# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
4.1.1.1           1   FULL/  -        00:01:52    10.0.1.5        Serial0
3.1.1.1           1   FULL/  -        00:01:52    10.0.1.4        Serial0
2.1.1.1           1   FULL/  -        00:01:52    10.0.1.3        Serial0
```

Variable-Length Subnet Masks Example

OSPF, static routes, and IS-IS support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which allows you to conserve IP addresses and more efficiently use available address space.

In the following example, a 30-bit subnet mask is used, leaving two bits of address space reserved for serial line host addresses. There is sufficient host address space for two host endpoints on a point-to-point serial link.

```
interface ethernet 0
 ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernets

interface serial 0
 ip address 131.107.254.1 255.255.255.252
! 2 bits of address space reserved for serial lines

! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
 network 131.107.0.0 0.0.255.255 area 0.0.0.0
```

OSPF Routing and Route Redistribution Examples

OSPF typically requires coordination among many internal routers, area border routers, and autonomous system boundary routers. At a minimum, OSPF-based routers can be configured with all default parameter values, with no authentication, and with interfaces assigned to areas.

Three examples follow:

- The first is a simple configuration illustrating basic OSPF commands.
- The second example illustrates a configuration for an internal router, ABR, and ASBRs within a single, arbitrarily assigned, OSPF autonomous system.
- The third example illustrates a more complex configuration and the application of various tools available for controlling OSPF-based routing environments.

CPMI - CORREIOS
Fls Nº 0418
3690

Basic OSPF Configuration Example

The following example illustrates a simple OSPF configuration that enables OSPF routing process 9000, attaches Ethernet 0 to area 0.0.0.0, and redistributes RIP into OSPF, and OSPF into RIP:

```
interface ethernet 0
 ip address 130.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 130.94.1.1 255.255.255.0
!
router ospf 9000
 network 130.93.0.0 0.0.255.255 area 0.0.0.0
 redistribute rip metric 1 subnets
!
router rip
 network 130.94.0.0
 redistribute ospf 9000
 default-metric 1
```

Basic OSPF Configuration Example for Internal Router, ABR, and ASBRs

The following example illustrates the assignment of four area IDs to four IP address ranges. In the example, OSPF routing process 109 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, while Area 0 enables OSPF for *all other* networks.

```
router ospf 109
 network 131.108.20.0 0.0.0.255 area 10.9.50.0
 network 131.108.0.0 0.0.255.255 area 2
 network 131.109.10.0 0.0.0.255 area 3
 network 0.0.0.0 255.255.255.255 area 0
!
! Interface Ethernet0 is in area 10.9.50.0:
interface ethernet 0
 ip address 131.108.20.5 255.255.255.0
!
! Interface Ethernet1 is in area 2:
interface ethernet 1
 ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet2 is in area 2:
interface ethernet 2
 ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet3 is in area 3:
interface ethernet 3
 ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet4 is in area 0:
interface ethernet 4
 ip address 131.109.1.1 255.255.255.0
!
! Interface Ethernet5 is in area 0:
interface ethernet 5
 ip address 10.1.0.1 255.255.0.0
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0419
Doc 3690

Each **network area** router configuration command is evaluated sequentially, so the order of these commands in the configuration is important. The Cisco IOS software sequentially evaluates the *address/wildcard-mask* pair for each interface. See the "OSPF Commands" chapter of the *Network Protocols Command Reference, Part 1* for more information.

Consider the first **network area** command. Area ID 10.9.50.0 is configured for the interface on which subnet 131.108.20.0 is located. Assume that a match is determined for interface Ethernet 0. Interface Ethernet 0 is attached to Area 10.9.50.0 only.

The second **network area** command is evaluated next. For Area 2, the same process is then applied to all interfaces (except interface Ethernet 0). Assume that a match is determined for interface Ethernet 1. OSPF is then enabled for that interface and Ethernet 1 is attached to Area 2.

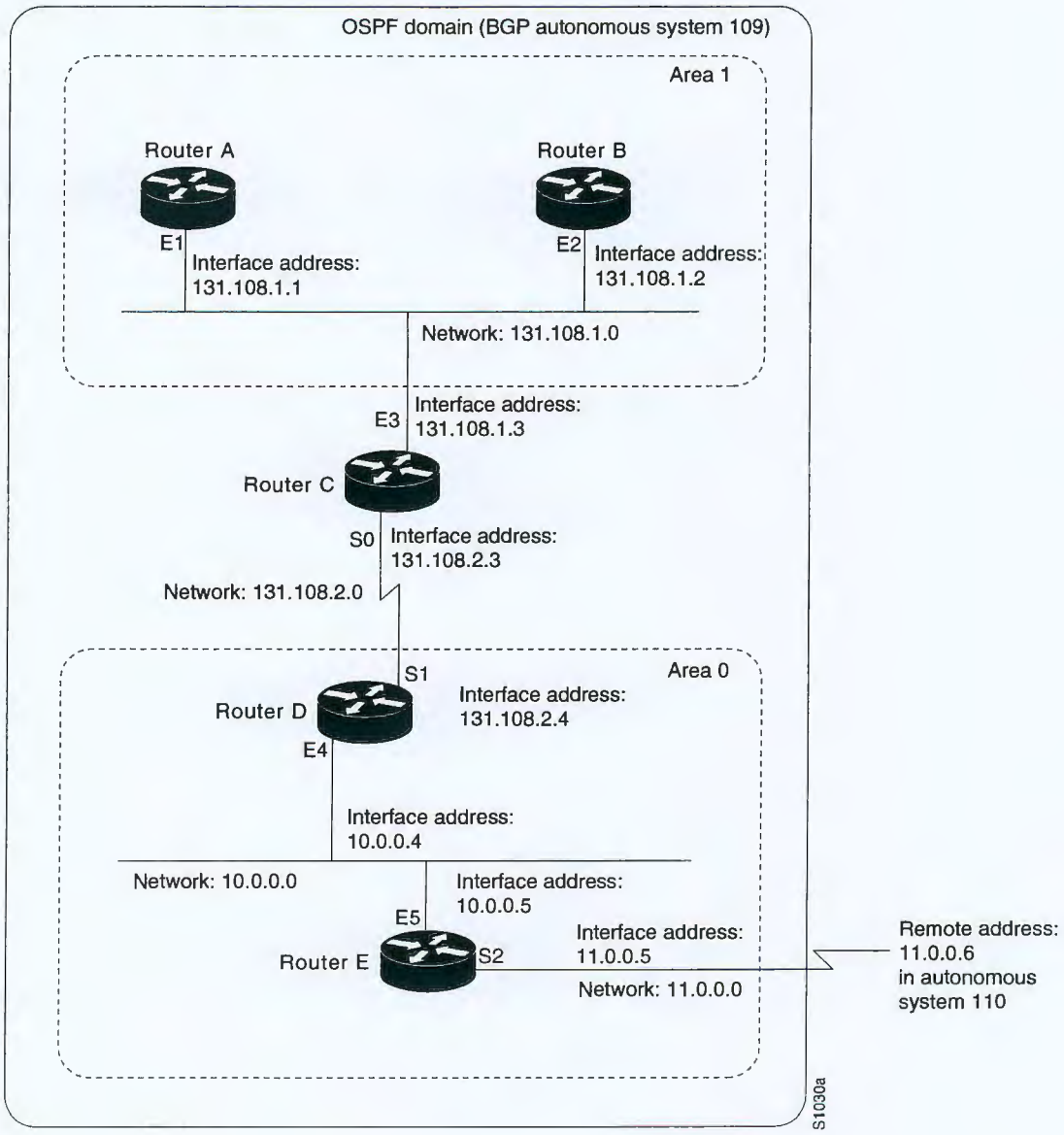
This process of attaching interfaces to OSPF areas continues for all **network area** commands. Note that the last **network area** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to Area 0.

Complex Internal Router, ABR, and ASBRs Example

The following example outlines a configuration for several routers within a single OSPF autonomous system. Figure 24 provides a general network map that illustrates this example configuration.

CPMI - CORREIOS
Fls Nº 0420
Doc. 3690

Figure 24 Sample OSPF Autonomous System Network Map



In this configuration, five routers are configured with OSPF:

- Router A and Router B are both internal routers within Area 1.
- Router C is an OSPF area border router. Note that for Router C, Area 1 is assigned to E3 and Area 0 is assigned to S0.
- Router D is an internal router in Area 0 (backbone area). In this case, both **network** router configuration commands specify the same area (Area 0, or the backbone area).
- Router E is an OSPF autonomous system boundary router. Note that BGP routes are redistributed into OSPF and that these routes are advertised by OSPF.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0421
Fls. Nº
Doc. 3690

Note It is not necessary to include definitions of all areas in an OSPF autonomous system in the configuration of all routers in the autonomous system. You must only define the *directly* connected areas. In the example that follows, routes in Area 0 are learned by the routers in Area 1 (Router A and Router B) when the area border router (Router C) injects summary link state advertisements (LSAs) into Area 1.

The OSPF domain in BGP autonomous system 109 is connected to the outside world via the BGP link to the external peer at IP address 11.0.0.6.

Router A—Internal Router

```
interface ethernet 1
 ip address 131.108.1.1 255.255.255.0

router ospf 1
 network 131.108.0.0 0.0.255.255 area 1
```

Router B—Internal Router

```
interface ethernet 2
 ip address 131.108.1.2 255.255.255.0

router ospf 202
 network 131.108.0.0 0.0.255.255 area 1
```

Router C—ABR

```
interface ethernet 3
 ip address 131.108.1.3 255.255.255.0

interface serial 0
 ip address 131.108.2.3 255.255.255.0

router ospf 999
 network 131.108.1.0 0.0.0.255 area 1
 network 131.108.2.0 0.0.0.255 area 0
```

Router D—Internal Router

```
interface ethernet 4
 ip address 10.0.0.4 255.0.0.0

interface serial 1
 ip address 131.108.2.4 255.255.255.0

router ospf 50
 network 131.108.2.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0422
Doc. 3690

14369

Router E—ASBR

```
interface ethernet 5
 ip address 10.0.0.5 255.0.0.0

interface serial 2
 ip address 11.0.0.5 255.0.0.0

router ospf 65001
 network 10.0.0.0 0.255.255.255 area 0
 redistribute bgp 109 metric 1 metric-type 1

router bgp 109
 network 131.108.0.0
 network 10.0.0.0
 neighbor 11.0.0.6 remote-as 110
```

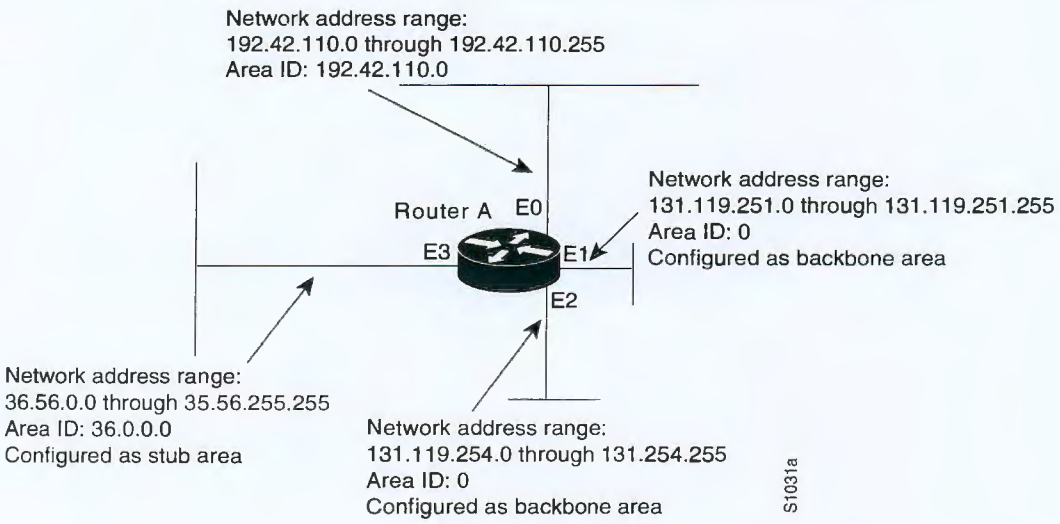
Complex OSPF Configuration for ABR Examples

The following example configuration accomplishes several tasks in setting up an ABR. These tasks can be split into two general categories:

- Basic OSPF configuration
- Route redistribution

The specific tasks outlined in this configuration are detailed briefly in the following descriptions. Figure 25 illustrates the network address ranges and area assignments for the interfaces.

Figure 25 Interface and Area Specifications for OSPF Example Configuration



The basic configuration tasks in this example are as follows:

- Configure address ranges for Ethernet 0 through Ethernet 3 interfaces.
- Enable OSPF on each interface.
- Set up an OSPF authentication password for each area and network.
- Assign link state metrics and other OSPF interface configuration options.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0423
Doc. 3690

- Create a *stub area* with area id 36.0.0.0. (Note that the **authentication** and **stub** options of the **area** router configuration command are specified with separate **area** command entries, but can be merged into a single **area** command.)
- Specify the backbone area (Area 0).

Configuration tasks associated with redistribution are as follows:

- Redistribute IGRP and RIP into OSPF with various options set (including **metric-type**, **metric**, **tag**, and **subnet**).
- Redistribute IGRP and OSPF into RIP.

The following is an example OSPF configuration:

```
interface ethernet 0
 ip address 192.42.110.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 1
 ip address 131.119.251.201 255.255.255.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf retransmit-interval 10
 ip ospf transmit-delay 2
 ip ospf priority 4
!
interface ethernet 2
 ip address 131.119.254.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 3
 ip address 36.56.0.201 255.255.0.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf dead-interval 80
```

OSPF is on network 131.119.0.0:

```
router ospf 201
 network 36.0.0.0 0.255.255.255 area 36.0.0.0
 network 192.42.110.0 0.0.0.255 area 192.42.110.0
 network 131.119.0.0 0.0.255.255 area 0
 area 0 authentication
 area 36.0.0.0 stub
 area 36.0.0.0 authentication
 area 36.0.0.0 default-cost 20
 area 192.42.110.0 authentication
 area 36.0.0.0 range 36.0.0.0 255.0.0.0
 area 192.42.110.0 range 192.42.110.0 255.255.255.0
 area 0 range 131.119.251.0 255.255.255.0
 area 0 range 131.119.254.0 255.255.255.0

 redistribute igrp 200 metric-type 2 metric 1 tag 200 subnets
 redistribute rip metric-type 2 metric 1 tag 200
```

PGS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0424
Doc. 3690

IGRP autonomous system 200 is on 131.119.0.0:

```
router igrp 200
 network 131.119.0.0
!
! RIP for 192.42.110
!
router rip
 network 192.42.110.0
 redistribute igrp 200 metric 1
 redistribute ospf 201 metric 1
```

Route Map Examples

The examples in this section illustrate the use of redistribution, with and without route maps. Examples from both the IP and CLNS routing protocols are given.

The following example redistributes all OSPF routes into IGRP:

```
router igrp 109
 redistribute ospf 110
```

The following example redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external link state advertisements with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
router ospf 109
 redistribute rip route-map rip-to-ospf
!
route-map rip-to-ospf permit
 match metric 1
 set metric 5
 set metric-type type1
 set tag 1
```

The following example redistributes OSPF learned routes with tag 7 as a RIP metric of 15:

```
router rip
 redistribute ospf 109 route-map 5
!
route-map 5 permit
 match tag 7
 set metric 15
```

The following example redistributes OSPF intra-area and interarea routes with next-hop routers on serial interface 0 into BGP with an INTER_AS metric of 5:

```
router bgp 109
 redistribute ospf 109 route-map 10
!
route-map 10 permit
 match route-type internal
 match interface serial 0
 set metric 5
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0425
Doc. 3690

The following example redistributes two types of routes into the integrated IS-IS routing table (supporting both IP and CLNS). The first are OSPF external IP routes with tag 5; these are inserted into Level 2 IS-IS LSPs with a metric of 5. The second are ISO-IGRP derived CLNS prefix routes that match CLNS access list 2000. These will be redistributed into IS-IS as Level 2 LSPs with a metric of 30.

```
router isis
 redistribute ospf 109 route-map 2
 redistribute iso-igrp nsfnet route-map 3
!
route-map 2 permit
 match route-type external
 match tag 5
 set metric 5
 set level level-2
!
route-map 3 permit
 match address 2000
 set metric 30
```

With the following configuration, OSPF external routes with tags 1, 2, 3, and 5 are redistributed into RIP with metrics of 1, 1, 5, and 5, respectively. The OSPF routes with a tag of 4 are not redistributed.

```
router rip
 redistribute ospf 109 route-map 1
!
route-map 1 permit
 match tag 1 2
 set metric 1
!
route-map 1 permit
 match tag 3
 set metric 5
!
route-map 1 deny
 match tag 4
!
route map 1 permit
 match tag 5
 set metric 5
```

The following configuration sets the condition that if there is an OSPF route to network 140.222.0.0, generate the default network 0.0.0.0 into RIP with a metric of 1:

```
router rip
 redistribute ospf 109 route-map default
!
route-map default permit
 match ip address 1
 set metric 1
!
 access-list 1 permit 140.222.0.0 0.0.255.255
 access-list 2 permit 0.0.0.0 0.0.0.0
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0426
3690
Doc.

In the following configuration, a RIP learned route for network 160.89.0.0 and an ISO-IGRP learned route with prefix 49.0001.0002 will be redistributed into an IS-IS Level 2 LSP with a metric of 5:

```
router isis
 redistribute rip route-map 1
 redistribute iso-igrp remote route-map 1
!
route-map 1 permit
 match ip address 1
 match clns address 2
 set metric 5
 set level level-2
!
 access-list 1 permit 160.89.0.0 0.0.255.255
 clns filter-set 2 permit 49.0001.0002...
```

The following configuration example illustrates how a route map is referenced by the **default-information** router configuration command. This is called *conditional default origination.* OSPF will originate the default route (network 0.0.0.0) with a Type 2 metric of 5 if 140.222.0.0, with network 0.0.0.0 in the routing table. Extended access-lists cannot be used in a route map for *conditional default origination.*

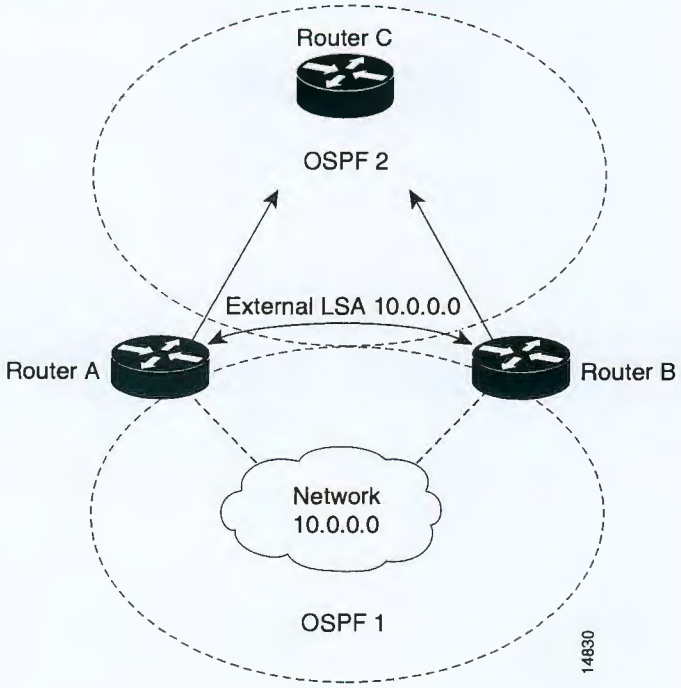
```
route-map ospf-default permit
 match ip address 1
 set metric 5
 set metric-type type-2
!
 access-list 1 140.222.0.0 0.0.255.255
!
router ospf 109
 default-information originate route-map ospf-default
```

Changing OSPF Administrative Distance

The following example changes the external distance to 200, making it less trustworthy. Figure 26 illustrates the example.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0427
Doc. 3690

Figure 26 OSPF Administrative Distance



Router A

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Router B

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

OSPF over On-Demand Routing Example

The following configuration allows OSPF over an on-demand circuit, as shown in Figure 27. Note that the on-demand circuit is defined on one side only (BRI 0 on RouterA). It is not required to be configured on both sides.

CORREIOS
Fls Nº 0428
Doc. 3690

Figure 27 OSPF over On-Demand Circuit

Router A

```
username RouterB password 7 060C1A2F47
isdn switch-type basic-5ess
ip routing
!
interface TokenRing0
 ip address 140.10.20.7 255.255.255.0
 no shut
!
interface BRI0
 no cdp enable
 description connected PBX 1485
 ip address 140.10.10.7 255.255.255.0
 encapsulation ppp
 ip ospf demand-circuit
 dialer map ip 140.10.10.6 name RouterB broadcast 61484
 dialer-group 1
 ppp authentication chap
 no shut
!
router ospf 100
 network 140.10.10.0 0.0.0.255 area 0
 network 140.10.20.0 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit
```

Router B

```
username RouterA password 7 04511E0804
isdn switch-type basic-5ess
ip routing
!
interface Ethernet0
 ip address 140.10.60.6 255.255.255.0
 no shut
!
interface BRI0
 no cdp enable
 description connected PBX 1484
 ip address  140.10.10.6 255.255.255.0
 encapsulation ppp
 dialer map ip 140.10.10.7 name RouterA broadcast 61485
 dialer-group 1
 ppp authentication chap
 no shut
!
router ospf 100
 network 140.10.10.0 0.0.0.255 area 0
 network 140.10.60.0 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
0429
Fls. Nº
3690
Doc.

LSA Group Pacing Example

The following example changes the OSPF pacing between LSA groups to 60 seconds:

```
router ospf
 timers lsa-group-pacing 60
```

Block LSA Flooding Example

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ospf database-filter all out
```

The following example prevents flooding of OSPF LSAs to point-to-multipoint networks to the neighbor at IP address 1.2.3.4:

```
router ospf 109
 neighbor 1.2.3.4 database-filter all out
```

Ignore MOSPF LSA Packets Example

The following example configures the router to suppress the sending of syslog messages when it receives MOSPF packets:

```
router ospf 109
 ospf ignore lsa mospf
```

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0430
3690
Doc.

RQS nº 03/2003 - CN
CPMI - CORREIOS
0431
Fls Nº
3690
Doc.

14360
20

Roteador Tipo 1 doc 11

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.- Nº 0432
Doc. 3690

Release Notes for ACL Manager 1.5 on Solaris and Windows

These release notes contain information on ACL Manager 1.5 running on Solaris and Windows. They provide the following information:

- New Features, page 1
- ACL Manager Documentation, page 2
- Supported Cisco IOS and Catalyst OS Releases, page 3
- Supported Devices, page 4
- Known and Resolved Problems, page 6
- Troubleshooting, page 22
- Obtaining Documentation, page 26
- Obtaining Technical Assistance, page 28

New Features

ACL Manager 1.5 has these new features that provide increased security and added functionality:

- Support for Secure Server to Device Communication Using IPSec
- Enhancements to the ACL Use Wizard
- Support for New Devices

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

PGS nº 03/2005 - CN
CPMI - - CORREIOS
0433
Fls Nº
3690
Doc.

Support for Secure Server to Device Communication Using IPSec

ACL Manager now supports IPSec for secure communication between server and device.

Enhancements to the ACL Use Wizard

You can now create ACLs out of a template, on multiple devices, using the ACL Use Wizard. If required, you can further apply such newly created ACLs to the selected interfaces of the devices.

It is no longer mandatory for you to create Uses for such ACLs, created from templates using the ACL Use Wizard, as it was in the previous release of ACL Manager.

Support for New Devices

This release supports new devices (see Table 1).
For a complete list of supported devices, see both Table 1 and Table 2, in the section "Supported Devices".

ACL Manager Documentation

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the ACL Manager documentation on Cisco.com for any updates.

The following documents are provided in PDF on your product CD:

- *Installation Guide for ACL Manager, Software Release 1.5*
- *User Guide for ACL Manager, Software Release 1.5*

Note Adobe Acrobat Reader 4.0 or later is required.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0434
Fls. Nº
3690
Doc.

Use these publications to learn how to install and use ACL Manager:

- *Installation Guide for ACL Manager* (DOC-7815203=)—Provides information about ACL Manager requirements and how to install the product.
- *User Guide for ACL Manager* (DOC-7815202=)—Provides information on using ACL Manager.
- *Release Notes for ACL Manager on Solaris and Windows* (DOC-7815142=)—Provides information on the new features, the supported devices and the known and resolved problems of ACL Manager 1.5, running on Solaris and Windows. It also provides troubleshooting information.
- ACL Manager online help—Contains all of the information available in *User Guide for ACL Manager*. This ensures you have complete information even if you do not have the manual readily available while using ACL Manager.

Additional Information Online

For answers to frequently asked questions about ACL Manager, see:

http://www.cisco.com/warp/public/cc/pd/wr2k/caclm/prodlit/aclm_qp.htm

You can download device packages for new devices from Cisco.com and find information about all supported devices by logging into Cisco.com.

Device packages are released cumulatively; that is, new device packages contain the contents of any previous packages.

To determine which packages are installed on your CiscoWorks Server, select **Server Configuration>About the Server>Applications and Versions**.

You can also obtain any published patches from the download site.

Supported Cisco IOS and Catalyst OS Releases

Support is provided for devices running Cisco IOS Releases 10.3 through 12.2 and Catalyst OS Releases 5.3 through 7.1.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0435
3690
Doc

Supported Devices

ACL Manager 1.5 newly supports the devices listed in Table 1.

Table 1 Newly Supported Devices in ACL Manager 1.5

Routers	Devices
Cisco 800 Series	827
Cisco 1700 Series	1721
Cisco 2600 Series	2691, 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM
Cisco 2900 Series	2950G-12-EI, 2950G-24-EI, 2950G-48-EI, 2950G-24-EI-DC
Cisco 3700 Series	3725, 3745
Catalyst 4000 series	4232 L3 module
Catalyst 4500 series	4503 (Supervisor III, IV), 4506 (Supervisor III, IV), 4507 (Supervisor IV)

Devices supported from the previous releases are in Table 2.

Table 2 Devices Supported From the Previous Releases

Routers	Devices
Cisco 800 Series	801, 802, 805
Cisco 900 UBR Series	UBR-904, UBR-905, UBR-924
Cisco 1000 Series	1000, 1003, 1004, 1005, 1020, CPA1003, CPA1004, CPA1005
Cisco 1600 Series	1601, 1602, 1603, 1604, 1605, CPA1601, CPA1602, CPA1603, CPA1604
Cisco 1700 Series	1710, 1720, 1750, 1751, 1760
Cisco 2400 series	IAD 2420
Cisco 2500 Series	2500 – 2525, 2501CF, 2501LF, 2502LF, 2509RJ, 2511RJ, CPA2500
Cisco 2600 Series	2610, 2611, 2612, 2613, 2620, 2621, 2650, 2651
Cisco 3600 Series	3620, 3640, 3660, CPA3640, CPA3620, 3661AC, 3661DC, 3662AC, 3662DC, 3662AC-CO, 3662DC-CO
Cisco 4000 Series	4000, 4000-M, 4500, 4500-M, 4700, 4700-M

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0436
3690
Doc.

Table 2 Devices Supported From the Previous Releases (continued)

Cisco 7xxx UBR Series	UBR-7246 VXR
Cisco 7000 Series	7000, 7010, 7120, 7140, 7200, 7202, 7204, 7204VXR, 7206, 7206VXR, 7505, 7506, 7507, 7507Z, 7507MX, 7513, 7513Z, 7513MX, 7576
Cisco 7300 series	7304
Cisco 7400 series	7401
Cisco 7600 series	7603, 7606, 7609 (7603, 7606, 7609 are also supported on hybrid images running CatOS.)
Cisco10000 ESR series	ESR-10005, ESR-10008
Cisco 10000 UBR Series	10012
Gigabit Switch Router Series	12004, 12008, 12012, 12016, 12404, 12406, 12416
Cisco switching access concentrator	MC3810
Cisco AS5000 Series	AS5200, AS5300, AS5800
Catalyst 2900-XL	2916M-XL, 2924-XL, 2924C-XL, 2924-XLv, 2924C-XLv, 2912-XL, 2924M-XL, 2912Mf-XL
Catalyst 2948G L3 Switch/Router	2948G-L3
Catalyst 2950	2950C-24
Catalyst 3550 Series	3550-12T, 3550-24, 3550-48
talyst 3500-XL	3508G-XL, 3512-XL, 3524-XL, 3548-XL, 3524T-XLEn
Catalyst 4000 series	4006 Supervisor III
Catalyst 5000	RSFC, RSM
Catalyst 6000	6006, 6009, 6509, 6506, 6509-NEBS, 6513, (all these switches running CatOS (Catalyst 6000 series switches running the native IOS are also supported.)
Catalyst 6000 MSFC	MSFC, MSFC II
Catalyst 8500	8510CSR, 8510MSR, 8515CSR, 8540CSR, 8540CSR with ACL Daughter card, 8540MSR with ACL Daughter card

CPMI - CORREIOS
Fls. Nº 437
3690
Doc.

Known and Resolved Problems

In this section, see:

Table 3—For the general known problems that occur in both Solaris and in Windows.

Table 4—For the known problems that are specific to device, IOS and Catalyst OS versions, in both Solaris and in Windows.

Table 5—For the known problems that are specific to downloads, in both Solaris and in Windows.

Table 6—For the known problems that occur specifically on Solaris.

Table 7—For the known problems that have been resolved since the last release of ACL Manager.

Note To obtain more information about known problems, access the Cisco Software Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. (You will be prompted to log into Cisco.com.)

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0438
3690
Doc
78-15142-01

Table 3 describes the general known problems that occur in both Solaris and Windows.

Table 3 General Known Problems

Bug ID	Description	Explanation
CSCdm02104	ACL Manager cannot be invoked as **http**://localhost	To connect to ACL Manager server, do not enter **http**://localhost (or http://127.0.0.1). Workaround: Use the local server's network IP address or name. For example, http://192.168.252.205, optionally with a port number.
CSCds05102	Expand ACE(s) Inline inserts comments in ACE column.	Expand Inline will expand any logical ACE into the physical equivalents of the ACE. Since each ACE may expand into multiple ACEs, the inline comments are duplicated at the beginning and the end of the newly generated list. Workaround: None.
CSCin06368	Use Wizard fails for SNMP Use if the Community string has a caret (^).	ACL Manager Use Wizard fails for SNMP Use if its Community string contains a special character, caret (^). For example, if you enter **asia^pacific** for the Community name, the name is split at the caret. As a result, `asia` incorrectly appears as the Community name and `pacific` as the View Name, in the Results window. Workaround: Do not enter a caret in the Community string for the Use Wizard.
CSCin08812	Cannot undo a deleted IP VACL.	You cannot undo the deletion of a Standard IP VACL. Workaround: None.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0439
Fls. Nº
3690
Doc.

Table 3 General Known Problems (continued)

Bug ID	Description	Explanation
CSCdm57940	Need a more accurate message when client gets disconnected from server.	If the client disconnects from the server, a message, `ORG.OMG.CORBA.NO_IMPLEMENT [completed=MAYBE]` appears. Workaround: None.
CSCin22741	Find does not work in Template Manager for ACEs	The Find option does not search for strings in ACEs within Template Manager. Workaround: None.
CSCin08814	Device does not appear when synchronizing to device on a TDU.	The Download Panel appears empty when you use the Sync Template on Device(s) option on a Template Device Use. This happens when the ACL contains expanded ACEs in place of a template. An ACL may contain expanded ACEs instead of a template when the download verify fails for the ACL that contains the template, and the device becomes stale. Workaround: None.
CSCdt20485	Fragments option is supported by CatOS 6.1 but not by ACLM	You cannot create an IP VACE using the Fragments option. Workaround: None.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0440
Doc 3690

Table 3 General Known Problems (continued)

Bug ID	Description	Explanation
CSCin18576	Issues with template tracking	The following are some of the issues with template tracking information (Template Device Uses or TDUs) in Template Manager: • Template Manager does not allow you to delete TDUs that have undergone Out-of-Band changes. When you refresh the device and use the Sync Template on Device(s) option, on such TDUs, the Downloader dialog box does not show these devices. • If you delete a template that is being used on some ACLs, and then select the Undo option, the template is restored, but its TDUs are deleted. The ACEs in which the template was used, appear as invalid. • If you make an Out-of-Band change on a device when the download of a modified ACL containing a template is in progress, the device in your scenario becomes stale. The TDU appears valid for this template. However, when you modify the template and use the Sync template on device(s) option, the TDU does not appear. • TDUs are not updated if a download is not attempted on a device. This may be because the ACLs present on the device are the same as those in the physical view. However, when you make a change, such as saving ACEs as a template, the Downloader dialog box indicates that the device configuration has changed. • If you select this device and download the job, the TDU for this device will not be updated in Template Manager.

CORREIOS
0441
3690

Table 3 General Known Problems (continued)

Bug ID	Description	Explanation
CSCin18576 (Continued)	Issues with template tracking (Continued)	• TDUs are not updated if you use Class Manager to update the Network Class or Service Class that is used in the template • When device configuration gets rolled back during job download (because of errors on this or other devices), ACL Manager may delete the TDU for the ACL on which the download failed. Workaround: • Modify the ACL to include template ACEs and schedule a job download. This will remove the invalid TDUs. or • Reschedule the old job containing the template. You can do this from the Job Browser dialog box of ACL Manager. To reschedule the job: a. Select the job that you want to re-submit. b. Click **Open** to open the scenario. c. Schedule download from the scenario. Since it is a read-only scenario, a message may appear that there were problems while removing the redundant ACEs. Ignore this message and proceed with scheduling the job. The invalid TDUs are removed. ⚠ **Caution** Do not use this method if you are not sure of all the changes made after scheduling this job. Since you are rolling back the configuration, this will remove all the logical changes done after the earlier job.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0442
Doc 3690

Table 3 General Known Problems (continued)

Bug ID	Description	Explanation
CSCin18576 (Continued)	Issues with template tracking (Continued)	Template Device Use (TDU) information is also lost under these circumstances: • If you restart the ACLM server when the job is in progress. • If the device becomes unreachable (because of wrong read community string or network problems) and if ACL Manager is restarted. • If you reboot the device when the startup and the running configurations are out of synchronization. • If you do not select Save to NVRAM when scheduling downloads to devices, TDU information is lost when you reboot the devices. Workaround: None.
CSCin26363	On a stale device, when you download an ACL that includes a template, the latest version of that template is not downloaded	On a stale device, if you download an ACL that includes a template, the latest version of the included templates does not get downloaded. As a result, the Template Device Use is displayed as False in ACL Manager, although the download was successful. Workaround: Refresh the stale device in your scenario and then download the ACL that includes a template, to the device. To refresh a stale device, see the section, Refreshing Devices, in the User Guide for ACL Manager. (On Cisco.com, select Products and Services > Network Management CiscoWorks > CiscoWorks Access Control List Manager > Version and Options > CiscoWorks Access Control List Manager 1.5 > User Guide for ACL Manager 1.5).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0443
3690
Doc.

Table 3 General Known Problems (continued)

Bug ID	Description	Explanation
CSCin40868	Problems with 2950 device support on ACLM	The following are some of the problems that occur in ACL Manager, with 2950 family of devices: • In the Properties of Device dialog box, the devices 2950-G12, 2950-G24 and 2950G-24-EI-DC(IOS version 12.1(9)EA1d) both dynamic and reflexive ACLs are incorrectly shown as Unsupported on the devices. • On the devices 2950-G12, 2950-G24 and 2950-G48 ACLs cannot be applied to outbound traffic on FastEthernet and GigabitEthernet interfaces. However, ACL Manager incorrectly allows you to apply ACLs, both in and out, on line interfaces and VLAN interfaces. • Time ranges cannot be applied to IP Extended ACLs on the device 2950-G48, although they can be created for these devices. However, ACL Manager incorrectly shows time-based ACLs as supported and also allows you to apply the time ranges. • For the 2950C-24 and 2950G-48 devices: – Standard IP logging and Extended IP logging are not supported on the device, but these are incorrectly shown as supported in the Properties of Device dialog box. – On the device, IP Extended ACLs can be created only with TCP, UDP, and IP protocols. However, ACL Manager allows all other protocols such as igrp, icmp, to be used. – Time-Ranges can be defined on the devices but you cannot associate them with ACLs. However, ACL Manager incorrectly allows you to associate time ranges with these devices.

RCS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0444
3690
Doc.

Table 3 General Known Problems (continued)

Bug ID	Description	Explanation
CSCin40868 (Continued)	Problems with 2950 device support on ACLM (Continued)	– TCP flags cannot be specified in an ACL on the devices. Tos/precedence, DSCP ACLs cannot be defined. – Reflexive ACLs and dynamic ACLs are not supported on the device. However, named IP ACLs, are displayed correctly. • The feature set for the 2950C-24 and 2950G-48 is displayed as unknown in the Properties of Device dialog box. Workaround: None.
CSCin40862	ACLM does not work through HTTP tunneling with proxy server	You cannot invoke ACL Manager if there is a proxy server and a firewall between the ACL Manager client machine and the CiscoWorks server. Workaround: Remove either the proxy server or the firewall.
CSCdt20501	ACLM does not work without Java Plug-in on Netscape.	This is cause by VisiBroker 2.5, which is shipped with Netscape 4.x by default. VisiBroker 2.5 classes are not compatible with VisiBroker 4.1 classes shipped with CiscoWorks. Workaround: Delete the file iiop10.jar from the Netscape 4.x installation. This file is located at: *Netscape Install Directory*\Program\java\classes.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0445
Fls. Nº
3690
Doc.

Table 4 shows the known problems that are specific to Device, IOS and Catalyst OS Versions. These problems occur both in Solaris and in Windows.

Table 4 Known Problems - Specific to Device, IOS, and Catalyst OS Versions

Bug ID	Description	Explanation
CSCdt67958	ACL Manager stops all traffic through interface.	ACL Manager stops all traffic through an interface when you download an access list whose first entry denies traffic through the interface. This happens when: • The interface is a management interface (an interface used by CiscoWorks to manage the device). or • It is an interface through which download traffic passes. In both cases, the ACL Use already exists on the interface for inbound traffic. Workaround: 1. On the device CLI, remove or modify the access list. If you have to modify the access list, ensure that proper connectivity has been established from the CiscoWorks machine to the device. **Warning** **This may allow unauthorized traffic, or may disallow authorized traffic for some duration.** 2. From ACL Manager, download the ACL again using TFTP download protocol.
CSCin09111	Can paste an ARP ACE from a Supervisor II device into a Supervisor I device.	ACL Manager allows you to incorrectly copy an ARP ACE from a device that supports ARP ACE (Supervisor II), and paste it into a device that does not support ARP ACEs, such as a Supervisor 1 device. Job download fails if such a VACL, containing an ARP ACE is downloaded to a device that does not support it. Workaround: None.

ECT nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 0446
3690
Doc.

Table 4 Known Problems - Specific to Device, IOS, and Catalyst OS Versions (continued)

Bug ID	Description	Explanation
CSCin09125	Applying VACL IP templates on interfaces, when SUP I and SUP II devices are selected, causes problems.	When you apply an IP VACL template, to an interface on a device, ACL Manager inserts an ARP VACE into the corresponding VACL that it creates, if the device is Supervisor II. When you select multiple devices, ACL Manager creates ARP VACEs for the VACLs on all the devices that you select. This may also include the devices that do not support ARP VACEs. In such a case, job download fails on these devices. Workaround: When you apply an IP VACL template to devices through the Use Wizard, for the correct behavior, select only the devices that support ARP VACEs, such as the Supervisor II device. Do not select together devices, such as Supervisor I and Supervisor II, and apply the template on their interfaces, as this will cause ACL Manager to insert ARP VACEs incorrectly.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0447
Doc 3690

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0448
Doc. 3690

Table 4 Known Problems - Specific to Device, IOS, and Catalyst OS Versions (continued)

Bug ID	Description	Explanation
CSCin09556	ACLM does not show ARP ACE, when upgraded from ACLM 1.4 or 1.3.	ACL Manager supports ARP ACEs on switches running CatOS 6.1 or higher with Supervisor II and PFC II. However, ACL Manager does not show ARP ACEs in the scenario, if you have upgraded from ACL Manager 1.4 or 1.3. Workaround: 1. Telnet to the device and change any of the configuration parameters on the device. For example, you can make a minor banner change. 2. Refresh the device. **Warning** **If you refresh the device, all the logical data, such as inline comments, templates, will be lost on the device.** After you refresh the device, the ARP ACEs appear in the scenario for Supervisor II devices (if you are running CatOS 6.1 and above).

CORREIOS
Fls N° 0449
3690

Table 4 Known Problems - Specific to Device, IOS, and Catalyst OS Versions (continued)

Bug ID	Description	Explanation
CSCin09556 (Continued)	ACLM does not show ARP ACE, when upgraded from ACLM 1.4 or 1.3. (Continued)	You can refresh the devices in the following ways: 1. Select ACL Manager > Edit ACLs from the Essentials Navigation tree. The Scenario Selection window appears. 2. Select the required scenario (that contains Supervisor II devices) and select the option ReadConfig from Device. 3. Click **Next**. The ACL Manager Main Window opens with your scenario containing the refreshed devices • If your ACL Manager Main Window is already open, you can select File > Open Scenario. You can select the required scenario from the Scenario Selection window, after checking the option, ReadConfig from Device. • If your scenario is already open in the ACL Manager Main Window, you can select View > Refresh Device, to refresh the devices from within your selected scenario.
CSCin06498	An ARP VACE does not appear in the physical view of a new IP VACL.	When you create a new IP VACL, the first entry is an ARP VACE. After creating the IP VACL, if you check the physical view (by selecting View > Physical View in the ACL Manager Main Window), the view does not show the ARP VACE. Workaround: 1. Recompute the physical view (by selecting View > Recompute Physical View in the ACL Manager Main Window) 2. Check the physical view again. The ARP VACE will be visible.

RQS nº 03/2005 - CN
CPMI - 0450
Fls Nº
Doc 3690

Table 4 Known Problems - Specific to Device, IOS, and Catalyst OS Versions (continued)

Bug ID	Description	Explanation
CSCin09039	ACLM does not recognize L3 interfaces for 3550s, 4006 Supervisor III and 6513	On 4006 Supervisor III, 3550 and 6513 devices running native IOS, you can convert Layer 2 interfaces to Layer 3 using the command **`no switchport`**. After the interfaces are converted, you can apply access lists on them. ACL Manager however, does not display these interfaces. It displays only the VLAN interfaces that are present on the device, and allows you only to apply ACLs on VLAN interfaces. Workaround: None.
CSCds20818	ACLM lists unsupported Ethertype for MAC VACLs.	The ethertype xerox-address-translation(0x0601) is not supported in MAC VACLs on some versions of CatOS. However, ACL Manager lets you select this option to create ACEs. This results in a download failure. Workaround: None.

RQS nº 03/2003 - CN
CPMI - CORREIOS
0451
Fls Nº
Doc: 3690

Table 5 shows the known problems that are specific to downloads. These problems occur both in Solaris and in Windows.

Table 5 Known Problems - Specific to Downloads

Bug ID	Description	Explanation
CSCdt67943	ACL Manager can cause failure of telnet and ftp sessions.	Traffic through a router can get affected when you apply a large ACL to a router interface, using ACL Manager. Workaround: None.
CSCds32898	Download fails if you include templates with options such as Capture and Fragments that are unsupported on the device.	When a template is included in an ACL, some properties of the device are not checked to ensure if the template is valid. For example, it does not check whether the device supports the new Fragments option (IP Extended ACL), or the Capture option (VACL). Workaround: None.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0452
Doc. 3690

Table 6 shows the known problems that occur specifically on Solaris.

Table 6 Known Problems - Specific to Solaris Operating System

Bug ID	Description	Explanation
CSCds40688	Some time zones are unsupported in Solaris with Common Services 2.2.	For these time zones, ACL Manager shows the time in GMT+0, whereas Essentials reports it as GMT+4: • PRC • GB • W-SU • Australia/North • Australia/Broken_Hill • Australia/Tasmania • Brazil/West Workaround: None.

Table 7 describes the problems resolved since the previous release of ACL Manager.

Table 7 Resolved Problems - Solaris and Windows

Bug ID	Summary	Additional Information
CSCin04763	Named ACLs cannot be used on 12*xxx* series interfaces.	Earlier, the download failed if you used named ACLs on the interfaces of the 12xxx series of devices. Although ACL Manager allowed you to use named ACLs on interfaces, the 12xxx series of devices did not allow you to use named ACLs on their interfaces. Job download failed in such cases. This problem is now resolved.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0453
Doc: 3690

Table 7 Resolved Problems - Solaris and Windows (continued)

CSCds34942	Hits Optimizer fails if device has XNS access-lists.	If the device configuration contained unsupported access-lists, such as XNS, Hits Optimizer did not work correctly. This problem is now resolved.
CSCin06514	TFTP does not work if an active Supervisor is in slot 2 of a Cat6K switch.	TFTP download did not work if the active Supervisor Card was present in slot 2 of a Catalyst 6000 series switch or a 7600 series switch, running Catalyst OS. This problem is now resolved.
CSCin09789	Telnet or TFTP options should not be selectable along with the Use SSH option.	ACL Manager supports SSH, Telnet and TFTP download protocols. Earlier, when different download protocols were selected, the following occurred: • For SSH: Use SSH and Use Telnet were both selected. • For Telnet: Only Use Telnet was selected. • For TFTP: Use TFTP was selected while Use SSH was either in the selected or the unselected state. However, these download protocols, SSH, Telnet and TFTP, did not have any interdependencies between them. This problem is now resolved.

RDS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0454
Doc. 3690

Table 7 Resolved Problems - Solaris and Windows (continued)

CSCds32970	Download verify fails if the only change is in the order of ACEs.	If you re-ordered the VACEs in a VACL and downloaded to a device, the download verification failed, because of a problem in Essentials Config Archive (see CSCds33989). This problem is now resolved.
CSCdw37774	Fragments option, TCP flags should not be selected together.	ACL Manager allowed you to incorrectly select the Fragments option along with a TCP flag. This problem is now resolved.

Troubleshooting

Table 8 Troubleshooting ACL Manager 1.5

Symptom	Probable Causes	Possible Solution
The ACL Manager Main Window is grayed out.	The OS did not refresh successfully.	Resize the ACL Manager Main Window to force refresh.
Template not visible in Template Selection Window	The Template Selection Window shows a list of Templates specific to the ACL Protocol. This means that if you are on ACL 100, you will see only IP Extended Templates and so on. However, Template Manager will list all templates. You should have administrator privileges to access Template Manager.	Create a template appropriate to the ACL protocol.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0455
Doc. 3690

Table 8 Troubleshooting ACL Manager 1.5 (continued)

Symptom	Probable Causes	Possible Solution
Error message: `Cannot connect to ACLM Server`	You tried to start Essentials or ACL Manager before the applications were initialized.	Wait 1 minute for Essentials and ACL Manager processes to start.
	TCP port 15349 is in use.	Use **`netstat -a -n`** to view status of TCP port 15349. If the port is in use, change the AclmPort value in aclm.properties.
	RmeGatekeeper is not running	To start RmeGatekeeper: 1. Select CiscoWorks Server > Administration > Process Management > Process Status. The Process Status dialog box appears. 2. Select RmeGatkeeper from the drop-down list box to start the process.
	The ACL Manager server is not running.	Select CiscoWorks Server > Administration > Process Management > Process Status to make sure the ACL Manager server is running.
	The JRM or Change Audit processes are not running.	Make sure JRM and Change Audit processes are running.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0456
Doc. 3690

Table 8 Troubleshooting ACL Manager 1.5 (continued)

Symptom	Probable Causes	Possible Solution
Download Job status: `Download Failed` Device Results reports that telnet credentials did not match.	Essentials telnet and enable passwords do not match device.	Match telnet and enable passwords in Essentials inventory with the device. From the CiscoWorks desktop, select Resource Manager Essentials> Administration > Inventory > Check Device Attributes. The Check Device Attributes dialog box appears. You can check the passwords, using this dialog box.
	TACACS username and password in Essentials do not match device.	If you are using TACACS, match the TACACS username and password in Essentials inventory with the device. Do not specify the local username and password in the Essentials inventory.
Download Job status: `Download Failed` Device Results reports that telnet could not get device prompt.	This happens if the device enable prompt ends in something other than #.	Set the device enable prompt to end in #.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0457
Fls. Nº
3690

Table 8 Troubleshooting ACL Manager 1.5 (continued)

Symptom	Probable Causes	Possible Solution
Download Job status: `Download Failed`. TFTP Download Failed and Device Results Reports SNMP Community string is wrong.	For TFTP download, ACL Manager uses SNMP Write Community string as well as SNMP Read Community string	Check that: • SNMP Write Community string has been updated in the Essentials Inventory. • Community strings are correct.
x minute delay while downloading console on Win2K.	On some Windows 2000 systems, the initial download of large Java applets (or subsequent downloads of the same applets that are not cached locally) might take longer than expected (up to 6 minutes in some instances). After the applet has been loaded and cached locally, the problem no longer occurs. The delay is caused by client side filtering mechanisms such as virus scanning. Some virus scanners are configured to automatically scan content downloaded by browsers. Scanning consumes a lot of memory and results in disk paging on most systems. Downloading is significantly slower than expected, because of this. (The effect is less on systems with large amounts of RAM and virtual memory.)	To enable a faster download: 1. Disable the automatic scanning of all downloaded files. 2. Enable the scanning of program files only (specified by file extension). Exact instructions vary depending on the virus scanner installed on your system. For more information, see the following article: http://support.microsoft.com/support/kb/articles/q240/3/09.asp

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0458
Doc 3690

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

RQS nº 03/2005 - CN
CPMI - CORREIOS
0459
Fls. Nº
3690
Doc.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can email your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0460
Doc 3690

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://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 levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

0461
Fls Nº
Doc. 3690

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- 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.

Cisco TAC Website

You can use the Cisco TAC website 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 website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/en/US/support/index.html

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 462
3690

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

Fls. Nº 0463
Doc. 3690

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

Fls. Nº 0464
Doc 3690

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the "ACL Manager Documentation" section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Release Notes for ACL Manager 1.5 on Solaris and Windows
Copyright © 2003 Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN
CPMI - 0465
Fls Nº
Doc. 3690

Roteador Tipo 1 doc 12

RQS nº 03/200
CPMI
0466
3690

Cisco Systems

Data Sheet

CiscoWorks Resource Manager Essentials 3.5

Resource Manager Essentials (RME) 3.5 is the cornerstone application of the CisocWorks family of network management solutions. LMS, RWAN and VMS all build on the intelligent facilities in RME that provide lifecycle management of Cisco network devices. Designed to reduce human error and eliminate many of the manual tasks associated with maintaining a network, RME helps make Cisco networks the most manageable and available in the world.

Resource Manager Essentials 3.5

RME 3.5 is a suite of tools for simplifying the administration of a Cisco network. These components include:

- Inventory Manager
- Device Configuration Manager
- Software Image Manager
- Change Audit Service
- Availability Manager
- Syslog Analyzer
- Cisco Management Connection
- Cisco Connection Online (CCO) Service Tools

RME Features Include

The basic purpose of RME is to simplify network operations and to dramatically simplify efficiency. RME can automate software updates and configuration changes, reduce human error, and track all devices and changes in the network.

Features include:

- Quickly builds a complete network inventory of Cisco devices
- Monitors and reports on hardware, configuration, and inventory changes
- Manages and deploys configuration changes and software image updates to multiple devices
- Simplifies monitoring and troubleshooting of critical local-area network (LAN) and wide-area network (WAN) resources
- Secure communication between the client browser and the server via Secure Sockets Layer (SSL) protocol.
- Secure upload/download of device configurations from server device via Secure Shell (SSH).

Inventory Manager—*Builds and maintains an up-to-date hardware and software inventory*

Inventory Manager provides an up-to-date inventory database of Cisco devices, from the Cisco 700 series Integrated Services Digital Network (ISDN) routers to the high-end CSS 11000, GSR 12400, and ESR 10000 series switches. The inventory database provides detailed inventory information on device attributes, such as chassis type, interfaces, software version, memory, Flash characteristics, and more. Inventory Manager provides a wide range of reporting capabilities from high-level summary reports to detailed device-level reporting.

Inventory Manager provides

0467
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Up-to-date inventory of all Cisco devices in the network, including support for Cisco CallManager, the VPN 3000 Concentrator (VPN c3000), CSS 11000, GSR 12400, and ESR 10000
- Hardware and software summary information as well as detailed reports for groups of devices, including device name, chassis type, memory, Flash, software version, interface, stack modules, and other detailed hardware and software characteristics
- Device import from Cisco WAN Manager as well as CWSI Campus 2.x, and Campus Manager 3.2, HP OpenView, Tivoli NetView, or from a flat file
- Capacity planning information by identifying the total number of free and used slots in many Cisco devices
- Multiservice port report on the number and location of Catalyst® switches that are multiservice port-enabled
- Device credentials (password information) that can be exchanged via Extended Markup Language (XML) with other management applications
- Ability to select VPN as a device grouping for report generation
- CLI command to extract Detailed Device Inventory information in XML format.
- Ability for Administrators to Title (ex Location, Owner etc.) the User Defined Fields. Inventory reports would reflect these titles.

Device Configuration Manager—*Maintains an active archive and simplifies deployment of configuration changes to multiple devices*

Device Configuration Manager consists of several sub-components: Configuration Archive, NetConfig, ConfigEditor & NetShow Applications.

Configuration Archive Benefits:

- Maintains an up-to-date archive by automatically identifying and storing changes to configuration files
- Supports configuration file searching to simplify locating specific device configurations and configuration attributes
- Identifies differences between the running and startup configurations
- Significant performance improvement over previous version (RME 3.4)
- Ability to choose a device and its version of configuration and download it to the device from the Config Archive application
- CLI command to extract Running Configuration of devices in XML format.

NetConfig

- Provides a wizard-based approach to simplify and reduce the complexities and time associated with rolling out global changes in the network
- NetConfig application allows configuration changes to be performed against multiple switches or routers in the network; changes can be downloaded immediately or run as scheduled operations
- Cisco-provided templates simplify the configuration change process for Simple Network Management Protocol (SNMP) community, Terminal Access Controller Access Control System (TACACS), enable, syslog, SNMP trap-destinations, Cisco Discovery Protocol (CDP), Domain Name System (DNS) and many others
- Flexibility in pushing command-line interface (CLI) changes out to the network via user-defined templates that are published to an authorized user or group of users for execution

ECT nº 03/2005 - CN
CPMI - CORREIOS
0468
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14324

- Support for downloading/uploading of device configurations Secure Shell (SSH) protocol (functionality also available in ConfigEditor & NetShow)
- Support for configuration management for devices across Network Address Translators (NAT) boundaries
- Support for Interactive IOS, CAT-OS and FastSwitch commands.
- Significant performance enchancements—up to X% faster than previous versions. (RME 3.4)
- Ability for operators to specify Username & Password for devices selected for the job, during job creation (functionality also available in ConfigEditor & NetShow)
- New Templates to Enable SSH & IPSec on devices

ConfigEditor

- ConfigEditor application provides a powerful Web-based editing facility for modifying and downloading configuration changes

NetShow

- Provides a simplified Web-based show command interface, allowing show commands to be run against multiple switches or routers to enhance and simplify network troubleshooting
- Batch interface to show commands, enabling multiple show commands to be run against a group of device as a scheduled operation

Software Image Manager—*Simplifies and speeds software image analysis and deployment*

Software Image Manager greatly simplifies the version management and routine deployment of software updates to Cisco routers and switches through wizard-assisted planning, scheduling, downloading, and monitoring of software updates. Software Image Manager automates the many time-consuming steps required to upgrade software images while reducing the error-prone complexities of the upgrade process. Built-in links to CCO correlate the Cisco online information about software patches with Cisco IOS and Catalyst software deployed in the network, highlighting related tech notes. New planning tools, also linked to CCO, find system requirements and send notification when hardware upgrades (Boot ROM, Flash RAM) are needed to support proposed software image updates.

Before an update is initiated, the prerequisites of a new image are validated against the target switch or router's inventory data to help ensure a successful upgrade. When multiple devices are being updated, Software Image Manager synchronizes download tasks and allows the user to monitor the progress of the job. Scheduled jobs are controlled through a signoff process, enabling managers to authorize a technician's activities before initiating each upgrade task. RME 3.5 includes the ability to analyze software upgrades for a wide range of Cisco routers and switches thereby greatly simplifying and reducing the time required to determine the impact of a software upgrade.

Software Image Manager benefits:

- Provides software update analysis reports showing prerequisites and impacts of proposed updates
- Reduces from hours to minutes the mean time to deploy router or switch software images
- Distributes single or multiple images to devices in a single deployment operation
- Support for software image management for devices across Network Address Translators (NAT) boundaries
- Performs network image software audits and software library synchronization
- Uses CCO to report on software defects and available patches that affect devices and images in your network
- Contains enhanced Web-proxy support for improved CCO connectivity
- Provides robust software upgrade analysis for Cisco devices

RQS nº 03/2005 - CN
CPMI - CORREIOS
0469
Fls Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Two new workflow models added to the Software Image Management Application
  - Ability for users to select an image, appropriate devices, followed by job scheduling. This new workflow reduces the amount of time it takes to create a job (especially if the image to be deployed is known), by eliminating the "Image Recommendation" phase.
  - This new workflow allows users to optimize bandwidth utilization by storing the image to be deployed on a router's flash and "instructing" the devices retrieve the image from the router.

Change Audit Service—*Displays comprehensive reports of software, hardware, and configuration changes*

Change Audit is a central point where users can view network changes. Summary information is easily displayed, showing the types of changes made, by whom and when, and whether the changes were made from a Telnet or console CLI or from a CiscoWorks application. Further, the nature of the changes is identified quickly through detailed reports (cards added/removed, memory changes, configuration changes, and so on). In organizations with policies defining when changes should be made to the network, Change Audit provides an exception summary, highlighting changes made outside the approved time window.

Change Audit benefits:

- Provides a comprehensive audit of network changes reported chronologically
- Records who changed what, when, and how
- Offers change report filtering using simple or complex sort criteria
- Identifies network changes made during critical network operational times

Availability Manager—*Highlights critical devices and their ability to respond*

Availability Manager's "reachability dashboard" quickly determines the operational status of critical routers and switches. From the availability monitor you can drill down on a particular device to view historical details about its response time, availability, reloads, protocols, and interface status.

Availability Manager benefits:

- Provides reports summarizing when critical devices went offline or reloaded
- Displays individual device drill-down views of reachability and availability history
- Offers graphical reports of device response time trends
- Features browser-accessible status reports of router and switch availability over time
- Provides connectivity to CCOs Stack Decoder to simplify reload failure troubleshooting
- Displays summaries of the protocols to which a device can respond (UDP, TCP, HTTP, TFTP, TELNET, SNMP) through the connectivity tool

Syslog Analyzer—*Isolates network error conditions and suggests probable causes*

Syslog Analyzer filters syslog messages logged by Cisco switches, routers, access servers, and Cisco IOS firewalls, displaying explanations of probable causes and recommended actions. It leverages embedded Cisco IOS technology to provide detailed device information. Its reports are based on user-defined filters that highlight specific errors or severity conditions and help identify when specific events occurred (such as a link-down on a device reboot). Syslog Analyzer allows syslog messages to be linked to customized information, such as Web-based administrative tips or to launch a Common Gateway Interface (CGI) script to take corrective actions.

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls Nº 0470
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Syslog Analyzer benefits:

- Speeds troubleshooting by displaying critical error patterns over time
- Summarizes syslog events by severity or user criteria for switches, routers, and Cisco IOS and PIX firewalls
- Supports selective filtering of remote syslog collectors, allowing only wanted messages to be sent to the RME server
- Separates unwanted messages with user-definable filters or scripts through local and remote filtering
- Launches user-defined scripts or links to a Web page for related information based on specific syslog messages
- New option to store messages that are scheduled to be purged from the database in a flat file.

Server, Client and Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions, and on Cisco's main on-line documentation site, under each CiscoWorks2000 solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco IOS Versions and Cisco Devices

http://cco/en/US/partner/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Availability

RME is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on the CiscoWorks family, see: http://cco/en/US/partner/products/sw/cscowork/index.html

To place an order, contact your local Cisco sales representative.

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203416/ETMG_03/03

DOU 07/05/03 - 01
Com. Cpmos
0471
Fls Nº
3690

14321

Roteador Tipo 1 doc 13

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0472
Doc. 3690

New and Changed Information

The following is a list of the new hardware and software features that are supported in Cisco IOS Release 12.3.

New Features in Release 12.3(1)

Documentation for new features that contain new or modified Cisco IOS software commands for Cisco IOS Release 12.3(1) can be found at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/index.htm

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL: http://www.cisco.com/register.

The following new features for Cisco IOS Release 12.3(1) are documented in these release notes only; these features do not contain new or modified Cisco IOS software commands.

New Hardware Features Supported in Cisco IOS Release 12.3(1)

The following are new hardware features supported in Cisco IOS Release 12.3(1).

- 1 and 2 Port Channelized T1/E1/PRI Network Module (NM-1CE1T1-PRI and NM-2CE1T1-PRI), page 123
- 1 port BRI S/T WAN Interface Card (WIC-1B-S/T-V2), page 124
- PA-POS-2OC3: 2-port Packet over SONET OC3c/STM1 Port Adapter, page 124
- VPN Acceleration Module 2 (VAM2), page 124

1 and 2 Port Channelized T1/E1/PRI Network Module (NM-1CE1T1-PRI and NM-2CE1T1-PRI)

The NM-1CE1T1-PRI (1-port) and NM-2CE1T1-PRI (2-port) network modules provide support for T1, E1, and ISDN primary rate interface (PRI) network connections in a network module form factor. This feature (referred to in this document as NM-xCE1T1-PRI) offers attachment of one T1, E1, or ISDN PRI line on the 1-port module and two T1, E1, or ISDN PRI lines on the 2-port version.

This new feature (NM-xCE1T1-PRI) enables you to configure a single network module as either a T1 interface or an E1 interface on the same card. The configuration of a T1 or E1 interface and the change from one to the other is controlled by the card type command. Additionally, when in E1 mode, the module can be configured between channelized E1, ISDN PRI, E1-CAS-R2, balanced and unbalanced, and structured (G.704) versus unstructured (G.703) modes. In T1 mode, the module can be configured for channelized T1, T1-CAS, and as a CSU/DSU.

CPMI - CORREIOS
Fls Nº 0473
Doc. 3690

Note After you insert the NM-xCE1T1-PRI feature network module into the router chassis, you must use the card type command in the command-line interface (CLI) to configure the NM-xCE1T1-PRI feature. The controller will not be detected and cannot be configured until you use the card type command.

The configuration of the T1 or E1 interface can be customized using command-line interface (CLI) commands. In E1 mode, each port can be individually set to 120-ohm or 75-ohm termination. Each port has RJ-48C connectors, and there is one bantam jack that is shared by each port (for 2-port cards) for monitoring.

1 port BRI S/T WAN Interface Card (WIC-1B-S/T-V2)

The new 1 port BRI S/T WAN Interface Card (WIC-1B-S/T-V2) provides one ISDN BRI port with an S/T interface. WIC-1B-S/T-V2 is a replacement for Cisco WIC-1B-S/T and provides all the functionality of the existing card.

PA-POS-2OC3: 2-port Packet over SONET OC3c/STM1 Port Adapter

The PA-POS-2OC3 provides two Packet-over-SONET (POS) ports in a single port adapter slot. The two ports function as either dual independent OC-3c/STM1 ports or a single port with automatic switchover. The PA-POS-2OC3 is used as a direct connection between the supported router or switch platform and external networks. The PA-POS-2OC3 fits into a single port slot on the Cisco 7204VXR, Cisco 7206VXR, Cisco 7401ASR router, and the Cisco 7500 series routers.

VPN Acceleration Module 2 (VAM2)

The Service Adapter VPN Acceleration Module 2 (SA-VAM2) is a single-width port adapter supported on Cisco 7200 series routers with the Network Processing Engine 225, 300, 400, G1 (NPE-225, NPE-300, NPE-400, NPE-G1), and the Network Services Engine (NSE-1) services accelerator.

An SA-VAM2 provides hardware-assisted tunneling and encryption services for Virtual Private Network (VPN) remote access, site-to-site intranets, and extranet applications, including security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management. The SA-VAM2 off-loads IPSec processing from the main processor to permit resources on the processor engines for other tasks.

New Software Features Supported in Cisco IOS Release 12.3(1)

The following are new software features supported in Cisco IOS Release 12.3(1).

- Service Independent Intercept, page 124
- T.38 Call Agent Driven Fax for Cisco IOS Voice Gateways, page 125

Service Independent Intercept

Service providers worldwide are legally required to allow government agencies to conduct surveillance on the service provider's traditional telephony equipment. The objective of the Service Independent Intercept feature is to enable service providers with New World networks to legally allow government agencies to conduct electronic surveillance on these New World networks (that is, conventional "wire tapping"). From a government agency perspective, you can see how this is important. Legislation and Regulation has been passed, or is being passed, in most countries worldwide to require service providers to support Lawful Intercept (LI).

LI is the term used to describe the process (not a specific regulatory requirement) by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order. Means and authority of conducting LI is often recorded in government legislation or regulatory mandates.

CPMI - CORREIOS
Fls Nº 0474
3690
Doc

T.38 Call Agent Driven Fax for Cisco IOS Voice Gateways

The T.38 Call Agent Driven Fax for Cisco IOS Voice Gateways feature enables T.38 fax relay interworking between H.323 gateways and MGCP gateways and between two MGCP gateways, under the control of a call agent. This feature introduces the ability for the gateway to accept the MGCP FXR package and to use the fxr prefix when communicating with the call agent. In addition, this feature introduces the ability for the gateway to accept a new port when switching from voice to fax transmission during a call.

This feature makes obsolete the CA-controlled mode as described in *Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay*. The CA-controlled mode described in that document used the ca parameter to communicate with the call agent, and the ca parameter is no longer supported as of Cisco IOS Release 12.3(1). That method for CA-controlled mode has been superseded by the method described in the current document. Note that the gateway (GW)-controlled mode described in the previous document remains supported and is the same as described in the *Cisco Fax Services over IP Application Guide*.

The T.38 Call Agent Driven Fax for Cisco IOS Voice Gateways feature is described in Chapter 4, "Configuring T.38 Fax Relay," in the *Cisco Fax Services over IP Application Guide*.

New Features in Release 12.3

Documentation for new features that contain new or modified Cisco IOS software commands for Cisco IOS Release 12.3 can be found at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123mindx/new123.htm

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL: http://www.cisco.com/register.

The following new features for Cisco IOS Release 12.3 are documented in these release notes only; these features do not contain new or modified Cisco IOS software commands.

New Hardware Features Supported in Cisco IOS Release 12.3

The following are new hardware features supported in Cisco IOS Release 12.3(1).

- 1 and 2-port T1/E1 Multiflex Voice/WAN Interface Card, page 127
- 1- and 2-Port V.90 Modem WICs for Cisco 1720, 1751, and 1760 Routers, page 127
- 1 Port Enhanced ATM Port Adapter with Support for 8K VCs, page 127
- 16-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series, page 127
- 1-Port T1/E1 Digital Voice Port Adapters for Cisco 7200 and Cisco 7500, page 127
- 36-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series, page 128
- 7100 PA Support, page 128

0475
Fls N°
3690

- 8-Port Mix-Enabled T1/E1/PRI PA, page 128
- ADSL over ISDN, page 129
- Analog Station Interface (ASI) Cards, page 129
- ATM OC-12 Port Adapter, page 129
- Catalyst 4224 Access Gateway Switch, page 129
- Catalyst 4500 Access Gateway Module 16-port RJ21 FXS Module (WS-U4604-16FXS), page 129
- Catalyst 4500 AGM Voice/WAN Bundle (WS-X4604-VOICE), page 129
- Cisco 1721 Router, page 130
- Cisco 1751 Router, page 130
- Cisco 1760 Router, page 130
- Cisco 2600XM Series Routers, page 130
- Cisco 2691 Series Router, page 130
- Cisco 3631 Router Enhanced Functionality, page 131
- Cisco 3631 Series Router, page 131
- Cisco 3640A Router, page 131
- Cisco 3725 Application Service Router, page 131
- Cisco 3725 Router, Cisco 3745 Router, Cisco 2691 Router Enhanced Functionality, page 132
- Cisco 3745 Application Service Router, page 132
- Cisco 7401 ASR-BB and Cisco 7401 ASR-CP, page 132
- Cisco 806 Broadband Gateway Router, page 132
- Cisco AS5350 Universal Gateway, page 132
- Cisco AS5850 Universal Gateway, page 133
- Cisco CVA122 Cable Voice Adapter, page 133
- Cisco CVA122E Cable Voice Adapter, page 133
- Cisco uBR905 Cable Access Router, page 133
- Cisco uBR925 Cable Access Router, page 133
- Gigabit Ethernet Network Module, page 134
- MRP300, page 134
- MRP3-16FXS, page 134
- MRP3-8FXS, page 134
- NPE-G1, page 134
- PA-MC-8TE1+, page 135
- RPM-XF Card for the MGX 8850, page 135
- SDH/STM-1 Trunk Card for Cisco AS5850 Universal Gateway, page 135
- Small Office, Home Office ADSL Router, page 135
- SRP MIB for DPT-OC12 WAN Card, page 135
- Update to the Enhancements for the Cisco Voice Gateway 200, page 135
- URM LAN, page 135

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0476
3690
Doc.

- VPN Encryption and Compression Module (AIM-VPN/EPII & AIM-VPN/HPII), page 136
- WIC-1-B-U-V2, page 136
- WT-2750 Multipoint Broadband Wireless System, page 136

1 and 2-port T1/E1 Multiflex Voice/WAN Interface Card

1- and 2-port T1/E1 Muliflex Voice/WAN interface cards provide basic structured and unstructured service for T1 or E1 networks. The card provides fractional data service and channelized voice services and TDM drop and insert (voice/data integration) services.

1- and 2-Port V.90 Modem WICs for Cisco 1720, 1751, and 1760 Routers

The one- and two-port V.90 Modem WICs expand the extensive range of WICs currently available on these routers. The modem WIC cards provide cost-effective basic telephone service connectivity to allow remote router management, asynchronous Dial-on-Demand routing (DDR) and dial back-up, and low-density remote access server (RAS) services.

1 Port Enhanced ATM Port Adapter with Support for 8K VCs

The PA-A6 is a series of single-width, single-port, ATM port adapters for Cisco 7200 series and Cisco 7401ASR routers. With advanced ATM features, the PA-A6 supports broadband aggregation, WAN aggregation, and campus/MAN aggregation.

16-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series

The16-Port Ethernet switch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The 16-port Ethernet switch network module has sixteen 10/100BASE-TX ports, and an optional power module can also be added to provide inline power for Cisco IP telephones.

Features included on this network module include the following:

- Broadcast/Multicast Suppression
- Classless InterDomain Routing (CIDR) IP Default Gateway
- IEEE 802.1Q ISL VLAN Mapping
- IEEE 802.1Q Tunneling
- IEEE 802.1Q VLAN Trunking
- IEEE 802.3x Flow Control
- MAC Address Filtering
- Spanning Tree Protocol-Backbone Fast Convergence
- Spanning Tree Protocol-Portfast Guard
- Spanning Tree Protocol-Uplink Fast Convergence
- Switch Port Analyzer (SPAN)
- Switch Port Analyzer (SPAN)—Disable Receive Traffic Destination Port
- Switch Port Analyzer (SPAN)—Multiple Source Port Selection
- Jumbo Frames

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0477
3690
Doc.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xt/122xt_2/ft1636nm.htm

1-Port T1/E1 Digital Voice Port Adapters for Cisco 7200 and Cisco 7500

The PA-VXB and the PA-VXC are multichannel packet voice port adapters that allow Cisco 7200 series routers, Cisco 7200 VXR routers, Cisco 7401ASR routers, and Cisco 7500 series routers to become dedicated packet voice hubs or packet voice gateways that connect to both private branch exchanges

(PBXs) and the Public Switched Telephone Network (PSTN). With this technology, packet voice and packet fax calls can be placed over the WAN and sent through the gateway into the traditional circuit-switched voice infrastructure. The PA-VXB and PA-VXC are single-width port adapters with two universal ports that are configurable for either T1 or E1 connections. The PA-VXB contains 12 high-performance digital signal processors (DSPs) that support up to 48 medium-complexity or 24 high-complexity channels of compressed voice. The PA-VXC contains 30 high-performance DSPs that support up to 120 medium-complexity or 60 high-complexity channels of compressed voice.

In Voice over IP (VoIP), the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. Because VoIP is a delay-sensitive application, you must have a well-engineered end-to-end network to use it successfully. Fine-tuning your network to adequately support VoIP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

36-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series

The 36-Port Ethernet switch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The 36-port Ethernet switch network module has thirty-six 10/100BASE-TX ports, and an optional power module can also be added to provide inline power for Cisco IP telephones.

The 36-port Ethernet switch network module supports the same features as the 16-port Ethernet switch network module introduced in Cisco IOS Release 12.2(8)T.

7100 PA Support

The 7100 PA is a port of support for the following features and port adapters on the Cisco 7100: Turbo ACLs, cRTP Acceleration, PA-GE, PA-MC-2T1, PA-MC-2E1/120, PA-POS, PA-MC-4T1, PA-MC-8T1, PA-MC-8E1, PA 2FE, PA-T3+, and PA-2T3+.

8-Port Mix-Enabled T1/E1/PRI PA

The PA-MC-8TE1+ port adapter is a single-wide port adapter that provides eight T1 or E1 interfaces for Cisco 7200 series routers. The PA-MC-8TE1+ interfaces can be channelized, fractional, or unframed (E1 only).

The PA-MC-8TE1+ provides the following features:

- Universal ports—Eight interface ports per port adapter are configurable as either T1 (with integrated channel service unit [CSU] and data service unit [DSU]) or E1 (with integrated G.703/G.704 balanced 120-ohm interface).
- Full DS0 channelization capability for all T1/E1 ports, for a maximum of 248 full-duplex HDLC channels.
- Data rates in multiples of 56 kbps or 64 kbps per channel.
- Maximum data rates per port: 1.536 Mbps (T1), 1.984 Mbps (E1 G.704), 2.048 Mbps (E1 unframed).
- Integrated T1/E1 supporting linecode AMI, B8SZ (T1), framing AMI or HDB3 (E1), framing SF or ESF (T1), CRC4, no-CRC4 or unframed (E1).
- Full Facility Data Link (FDL) support and FDL performance monitoring per-ANSI T1.403 or AT&T TR 54016.
- Full ISDN support for either 23B+D (T1) or 30B+D via network processing engine (NPE).
- Performance monitoring.
- Alarm integration, detection, and insertion.
- Line and payload loopback on a per-DS0 level.
- BERT functionality to transmit and receive test patterns over any Nx64 channel group.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0478
3690

- Clock jitter attenuators.
- Line or internal clocking.

Refer to the *PA-MC-8TE1+ Port Adapter Installation and Configuration Note* for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/multicha/8port_t1/index.htm

ADSL over ISDN

Cisco 826 routers connect corporate telecommuters and small offices via Internet Service Providers (ISPs) over asymmetric digital subscriber lines (ADSLs) to corporate LANs and the Internet. The router can provide bridging and multiprotocol routing between LAN and WAN ports. Cisco 826 routers provide connectivity to an ISDN network through an ADSL port.

Analog Station Interface (ASI) Cards

Analog station interface (ASI) cards enable you to connect to analog telephones, fax machines, and teleconferencing stations. The following two ASI cards are available:

- ASI 81—Contains an 8-port Foreign Exchange Station (FXS) module and any one of the VIC/WIC/VWIC modules that support digital and analog voice trunks and WAN routing interfaces, completely integrating voice and data networking.
- ASI 160—Contains a 16-port FXS module.

ATM OC-12 Port Adapter

Platforms: Cisco 7500/RSP series with Versatile Interface Processor (VIP)

The ATM OC-12 Port Adapter is a dual-width ATM port adapter that provides a single-port, 622.08 Mbps connection from Cisco 7500 series routers to any ATM switch. The PA-A3 OC-12 includes two hardware versions (PA-A3-OC12MM and PA-A3-OC12SMI) that support the following standards-based physical interfaces:

- OC-12c/STM-4 multimode
- OC-12c/STM-4 single-mode intermediate reach

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/6228oc12/6228ovrn.htm

Catalyst 4224 Access Gateway Switch

The Cisco Catalyst 4224 Access Gateway Switch (Catalyst 4224) is an integrated switch/router that provides Voice over IP (VoIP) gateway and IP telephony services to a small branch office. The Cisco Catalyst 4224 provides an integrated switch and WAN/voice gateway for enterprise satellite offices with up to 24 users. It is intended to work in conjunction with a Cisco Call Manager cluster from the central site with fail over capabilities to allow local calls and basic PBX features.

For information about Cisco Catalyst 4224 configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4224/index.htm

Catalyst 4500 Access Gateway Module 16-port RJ21 FXS Module (WS-U4604-16FXS)

The 16-Port RJ21 FXS module for the Catalyst 4500 Access Gateway Module is a high density analog phone and fax interface. By providing service to analog phones and fax machines, the sixteen Foreign Exchange Station (FXS) ports emulate a PSTN central office (CO) or PBX.

Catalyst 4500 AGM Voice/WAN Bundle (WS-X4604-VOICE)

The Cisco Catalyst 4500 AGM Voice/WAN bundle provides integrated telephony and routing services to the Cisco Catalyst 4000 series and Cisco Catalyst 4500 series switches. The Cisco Catalyst 4500 AGM Voice/WAN bundle consists of the following products:

- Cisco Catalyst 4500 Access Gateway Module (WS-X4604-GWY)

CPMI - CORREIOS
Fls 0479
3690
Doc.

- Cisco Catalyst 4500 AGM 96-channel Digital Signal Processor Set (4x6 DSP SIMMS) (WS-X4604-DSP)
- Cisco Catalyst 4500 AGM 128-MB RAM DIMM (MEM-C4K-AGM128M)

Cisco 1721 Router

The Cisco 1721 data-only modular access router is an enhanced Cisco 1720 router that provides higher performance, additional functionality, and increased memory capacity. The router supports WAN access, Virtual Private Network (VPN), and firewall technology for secure Internet, intranet, and extranet access. Cisco 1721 routers also support standards-based Institute of IEEE 802.1Q VLAN routing, which enables enterprises to set up and route between multiple VLANs for additional security in an internal corporate network.

Cisco 1751 Router

The voice-and-data capable Cisco 1751 router provides global Internet and company intranet access and includes the following:

- Voice-over-IP (VoIP) voice-and-data functionality; the router can provide support for digital and analog voice traffic (for example, telephone calls and faxes) over an IP network.
- Support for virtual private networking.
- Modular architecture.
- Network device integration.

Cisco 1760 Router

The Cisco 1760 router is a voice-and-data-capable router that provides Voice-over-IP (VoIP) functionality and can carry voice traffic (for example, telephone calls and faxes) over an IP network. Using one or two WAN connections, the router links small-to-medium-size remote Ethernet and Fast Ethernet LANs to central offices.

The Cisco 1760 router is available in two models. The Cisco 1760 runs data and data-plus-voice images, providing digital and analog voice support. The Cisco 1760-V includes all the features needed for immediate integration of data and voice services with support for multiple voice channels.

Refer to the documents at the following location for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm

Cisco 2600XM Series Routers

The Cisco 2600XM series provides new product enhancements to the current Cisco 2600 series. The Cisco 2600XM series is available in three performance levels and six base configurations:

- Cisco 2650XM and Cisco 2651MX—up to 40K packets per second (pps), one and two autosensing 10/100 Mbps Ethernet ports.
- Cisco 2620XM and Cisco 2621XM—up to 30K pps, one and two autosensing 10/100 Mbps Ethernet ports.
- Cisco 2610XM and Cisco 2611XM—up to 20K pps, one and two autosensing 10/100 Mbps Ethernet ports.

Each model also has two WAN interface card (WIC) slots, one Network Module slot, and an Advanced Integration Module.

Cisco 2691 Series Router

The Cisco 2691 router is part of the next generation Modular Multiservice platform for deployment of advanced IP Telephony Solutions and Integrated Services. This platform is the fourth in a series of Cisco 2600 products that offer additional performance levels.

CPMI CORREIOS
0480
Fls Nº
3690
Doc.

The Cisco 2691 provides two 10/100BASE-T Fast Ethernet (FE) ports with one Network Module (NM) slot, three WAN Interface Cards (WICs) slots, and two Advanced Interface Module (AIM) slots. Many of the current NMs, WICs and AIMs used today on the Cisco 2600 and Cisco 3600 series routers are supported on the Cisco 2691 series router.

Cisco 3631 Router Enhanced Functionality

The Cisco 3631 supports the following interfaces:

- NM-T3
- NM-E3
- NM-1FE2W
- NM-2FE2W
- NM-2W
- NM-8B-S/T
- NM-8B-U
- NM-1CEB
- NM-1CEU
- NM-2CEB
- NM-2CEU
- ETM

For more information about network module configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

For more information about WAN interface card (WIC) configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/index.htm

Cisco 3631 Series Router

The Cisco 3631 is a new midrange router for Data Communication Network (DCN) applications that provides two network modules and two WICs, one Fast Ethernet port, one console port, and an auxiliary port. The Cisco 3631 is two rack units high in an 11-inch NEBS/ETSI-compliant chassis that functions at 70,000 pps.

Cisco 3640A Router

The Cisco 3640A is identical to the Cisco 3640 router in terms of physical characteristics, interface support, performance and memory. The Cisco 3640A router will support the same Cisco IOS feature sets as the Cisco 3640 router, but requires a different minimum version of Cisco IOS software.

Cisco 3725 Application Service Router

The Cisco 3725 Series Application Service Router is part of a new family of modular routers that enable flexible and scalable deployment of new e-business applications in an integrated branch office access platform.

The Cisco 3700 series are new access platforms optimized for the modular integration and consolidation of branch applications and services. The Cisco 3725 is a two-rack unit (RU) router equipped with two on-board Fast Ethernet (FE) interfaces, three WAN Interface Card (WIC) slots and two Advanced Integration Module (AIM) slots, and two network module (NM) slots. The Cisco 3725 also includes optional –48VDC integrated inline power to support IP Telephony when used with an EtherSwitch network module.

0481
Fls Nº
3690

Cisco 3725 Router, Cisco 3745 Router, Cisco 2691 Router Enhanced Functionality

The Cisco 3725, Cisco 3745, and Cisco 2691 routers will support the following interfaces:

- AIM-ATM
- AIM-VOICE-30
- AIM-ATM-VOICE-30
- AIM-VPNII
- OC-3 NMs (Multimode, Singlemode Intermediate Reach and Singlemode Long Reach)
- WIC-1SHDSL
- VIC-2BRI-NT/TE

For more information about network module configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

For more information about WAN interface card (WIC) configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/index.htm

Cisco 3745 Application Service Router

The Cisco 3745 Series Application Service Router is part of a new family of modular routers that enable flexible and scalable deployment of new e-business applications in an integrated branch office access platform.

The Cisco 3745 is a three-rack unit (RU) router equipped with two on-board Fast Ethernet (FE) interfaces, three WAN Interface Card (WIC) slots and two Advanced Integration Module (AIM) slots, and two network module (NM) slots. The Cisco 3745 also includes optional 48vDC integrated inline power, internal redundant AC or DC Power options, and Online Insertion and Removal (OIR) capabilities for like network modules.

The Cisco 3700 series is ideal for sites and solutions requiring the highest levels of integration at the edge, such as:

- Integration of flexible routing and low density switching.
- Single platform solution for Branch Office IP Telephony and Voice Gateway allowing flexible, incremental migration and service integration.
- Consolidation of service infrastructure and high service density in a compact form factor.

Cisco 7401 ASR-BB and Cisco 7401 ASR-CP

The Cisco 7401 ASR-BB and Cisco 7401 ASR-CP are supported in Cisco IOS Release 12.3.

Cisco 806 Broadband Gateway Router

The Cisco 806 Broadband Gateway Router adds business-class functionality to affordable broadband access for small offices and corporate telecommuters. Through the power of Cisco IOS technology, the Cisco 806 provides business-class security, remote management, and quality of service capabilities. These value-added features, with the proven reliability of Cisco IOS technology, provide the mission-critical networking required by today's agile businesses.

Cisco AS5350 Universal Gateway

The Cisco AS5350 Universal Gateway is the only one-rack-unit, two, four, or eight PRI gateway that provides universal services—data, voice, and fax services on any service, any port. The Cisco AS5350 offers high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprises that require innovative universal services.

CORREIOS
Fls. Nº 0482
3690

Refer to the documents at the following location for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm

Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway provides the highest concentration of port and Integrated Services Digital Network (ISDN) terminations available in a single remote access server product. The Cisco AS5850 is specifically designed to meet the demands of large service providers such as Post, Telephone, and Telegraphs (PTTs), regional bell operating companies (RBOCs), inter-exchange carriers (IXCs), and large Internet service providers (ISPs).

Refer to the documents at the following location for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/index.htm

Cisco CVA122 Cable Voice Adapter

The Cisco CVA122 Cable Voice Adapter acts as a cable modem to connect computers and other customer premises equipment (CPE) devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network. The Cisco CVA122 Cable Voice Adapter is based on the Data-over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified cable modem termination system (CMTS).

The Cisco CVA122 Cable Voice Adapter supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network. PCs and other CPE devices can connect to the cable voice adapter either through an Ethernet port or through a Universal Serial Bus (USB) port. Single-line telephones, fax, or modems can be connected to two RJ-11 analog voice ports of the cable voice adapter. The cable voice adapter supports DOCSIS-compliant bridging data operations, and it can also function as an advanced router, providing WAN data and VoIP connectivity in a variety of configurations.

Cisco CVA122E Cable Voice Adapter

The Cisco CVA122E Cable Voice Adapter acts as a cable modem to connect computers and other customer premises equipment (CPE) devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network. The Cisco CVA122E Cable Voice Adapter is based on the European Data-over-Cable Service Interface Specifications (EuroDOCSIS) and interoperates with any bidirectional, EuroDOCSIS-qualified cable modem termination system (CMTS).

The Cisco CVA122 Cable Voice Adapter supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network. PCs and other CPE devices can connect to the cable voice adapter either through an Ethernet port or through a Universal Serial Bus (USB) port. Single-line telephones, fax, or modems can be connected t o two RJ-11 analog voice ports of the cable voice adapter. The cable voice adapter supports EuroDOCSIS-compliant bridging data operations, and it can also function as an advanced router, providing WAN data and VoIP connectivity in a variety of configurations.

Cisco uBR905 Cable Access Router

The Cisco uBR905 Cable Access Router features a single F-connector interface to the cable system, four RJ-45 (10BASE-T Ethernet) hub ports, and one RJ-45 console port to connect to a laptop computer/console terminal for local Cisco IOS configuration. The Cisco uBR905 Cable Access Router also provides an onboard IPSec hardware accelerator, which provides high-performance encryption that is substantially faster than software-based encryption.

Cisco uBR925 Cable Access Router

The Cisco uBR925 cable access router acts as a cable modem to connect computers and other customer premises equipment (CPE) devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network. The Cisco uBR925 router is based on the Data-over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified cable modem termination system (CMTS).

The Cisco uBR925 cable access router supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network. PCs and other CPE devices can connect to the Cisco uBR925 router either through a four-port Ethernet hub or through the Universal Serial Bus (USB) port of the router. Single-line telephones, fax, or modems can be connected to two RJ-11 analog voice ports of the router. The Cisco uBR925 router supports DOCSIS-compliant bridging data operations, and it can also function as an advanced router, providing WAN data and VoIP connectivity in a variety of configurations.

Gigabit Ethernet Network Module

The Gigabit Ethernet (GE) network module provides gigabit connectivity. The throughput of the interface depends on the platform. The network module has one GBIC slot to carry any standard copper or optical Cisco GBIC, including CWDM. The GE network module optimizes the performance for branch office customers by offering a high-speed uplink to both existing and new LAN or WAN environments. The extended reach of the provided fiber connectivity allows customers the option of interconnecting branch offices with Gigabit Ethernet and avoids expensive leased serial lines. Metro area service providers now have additional options when connecting their customers in branch offices to MANs.

The Gigabit Ethernet network module is supported on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.

MRP300

The Multiservice Route Processor 300 (MRP300) is a voice-and-data-capable router that can carry voice traffic over an IP network and that can link small-to-medium-size remote Ethernet LANs to central offices over WAN links. The MRP300 has a slot for expanding flash memory; two slots that support WICs, VWICs, and VICs; two PVDM slots for adding DSPs; and a DIMM slot for upgrading DRAM.

MRP3-16FXS

The MRP3-16FXS contains a 16-port Foreign Exchange Station (FXS) module. The MRP3-16FXS is similar to the analog station interface 161 card (ASI160), except that the ASI160 does not have onboard Flash memory.

MRP3-8FXS

The MRP3-8FXS contains an 8-port Foreign Exchange Station (FXS) module and a slot for any VIC, WIC, or VWIC module that supports digital and analog voice trunks and WAN routing interfaces. The MRP3-8FXS is similar to the analog station interface 81 card (ASI81), with the exception that the ASI81 does not have onboard Flash memory.

NPE-G1

The NPE-G1 is the first network processing engine for the Cisco 7200 VXR routers to provide the functionality of both a network processing engine and an I/O controller. If used without an I/O controller, an I/O blank panel must be in place.

Although its design provides I/O controller functionality, it can also work with any I/O controller supported in the Cisco 7200 VXR routers. The NPE-G1, when installed with an I/O controller, provides the primary input/out functionality; that is, the NPE-G1 input/out functionality enhances that of the existing I/O controller. However, when both the I/O controller and NPE-G1 are present, the functionality of the auxiliary port and console port are on the I/O controller.

The NPE-G1 maintains and executes the system management functions for the Cisco 7200 VXR routers and also holds the system memory and environmental monitoring functions.

The NPE-G1 consists of one board with multiple interfaces. It is keyed so that it can be used only in the Cisco 7200 VXR routers.

ROS nº 03/2005 - CN
CPMI - Correios
0484
Fls Nº
3690
Doc.

PA-MC-8TE1+

The Cisco PA-MC-8TE1+ is a single-wide port adapter designed to provide a full eight-port PRI multichannel solution for the Cisco 7200 and Cisco 7400. The interfaces can be channelized, fractional or ISDN-PRI, or unframed (E1) with up to 256 independent HDLC channels definable for T1 and E1 applications.

RPM-XF Card for the MGX 8850

The RPM-XF card is a next-generation, high-performance model of the RPM for the MGX 8850 platform, using PXM45 processor modules. It is a router module based on an RM7000A MIPS processing engine.

The RPM-XF hardware provides forwarding technology for packet switching capabilities in excess of 2-million pps. The forwarding engine is packet based and is interfaced to the midplane of the system through a combination of switch interface technologies.

SDH/STM-1 Trunk Card for Cisco AS5850 Universal Gateway

Channelized STM-1 provides a high speed remote access aggregation solution with 63 E1s and 1890 DSO channels. The SDH/STM-1 trunk card is a high density mux/demux card that takes in an STM-1 (SDH) pipe, used to transport up to 1890 DS0 channels. The SDH/STM-1 trunk card provides an ingress connection between the Cisco AS5850 universal gateway and external networks. The SDH/STM-1 trunk card has a 155-Mbps channelized SDH physical interface in a standard dial feature card (DFC) format. The SDH interface supports channelization to 64 kbps and connects to single mode fiber optic supporting intermediate reach PPP applications.

Small Office, Home Office ADSL Router

Cisco IOS Release 12.3 supports the following Cisco SOHO series routers:

- SOHO 76
- SOHO 77

The SOHO 76 and SOHO 77 are small office, home office (SOHO) asymmetric digital subscriber line (ADSL) routers, each with one Ethernet interface for connection to service provider networks.

The SOHO routers also provide the following key hardware features:

- Connection to an ADSL network through an ADSL port.
- A central processing unit: 50 MHz MPC 855T RISC processor.
- Ability to be stacked or mounted on a wall.
- Locking power connectors and a Kensington-compatible locking slot.

SRP MIB for DPT-OC12 WAN Card

This feature provides the SRP MIB for PA-SRP-OC12xx and SRPIP-OC12xx cards for the Cisco 7200 and Cisco 7500 series routers.

Update to the Enhancements for the Cisco Voice Gateway 200

The Enhancements for the Cisco Voice Gateway 200 (Cisco VG200) feature provides the Cisco VG200 platform (also called CAG-VG200) with increased voice gateway feature parity to the Cisco 2600, Cisco 3600, and Cisco 3700 platforms. This update provides additional feature functionality on the Cisco VG200 platform.

The Cisco VG200 platforms provide the following default memory options: 16 MB of Flash, 64 MB of DRAM.

URM LAN

On the Cisco IGX 8400 series, the Universal Router Module (URM) has been enhanced by new LAN features such as Security and VPN. Installed URMs can be enabled with the new features by upgrading to IGX switch software 9.3.30 and Cisco IOS Release 12.2(2)XX as well as by adding an AIM-VPN

CPMI - CORREIOS
Fls Nº 0485
3690

daughter module to the URM. Also, a new, price-reduced back card for the URM with 2 FE ports (BC-URI-2FE) for LAN services will be supported. URM together with the voice-enabled back cards (BC-URI-2FE2V-E1/T1) will support the new LAN.

VPN Encryption and Compression Module (AIM-VPN/EPII & AIM-VPN/HPII)

The VPN Encryption AIM provides hardware-based DES/3DES/AES and Compression services for Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 routers. The Data Compression supports IPSec IPPCP and supports the industry standard LZS. For more information about configuring the virtual private network (VPN) encryption hardware advanced integration modules (AIM-VPN/EPII & AIM-VPN/HPII) and network modules, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftaimvpn.htm

WIC-1-B-U-V2

Beginning in this release, the model number for the existing WIC-1-B-U interface card for the Cisco 1700 series, Cisco 2600 series, and Cisco 3600 series is changing to WIC-1-B-U-V2.

In addition, this interface card will now be supported on the Cisco 1760, Cisco 2691, Cisco 3725, and Cisco 3745 beginning with this release.

T-2750 Multipoint Broadband Wireless System

The Cisco broadband fixed wireless point-to-multipoint system is an integrated solution consisting of one headend (WT-2751 Multipoint Headend Line Card) and multiple subscriber units (WT-2755 Multipoint Subscriber Network Module). The fixed wireless point-to-multipoint subscriber unit is designed to receive radio frequency (RF) signals from the headend. It also transmits a return signal to the headend. This return signal is a point-to-point signal, so a properly installed subscriber antenna must be correctly oriented with the headend antenna to which it is transmitting.

For more information about the fixed wireless point-to-multipoint headend feature, refer to *Point-to-Multipoint Support for the Cisco uBR7200 Series Universal Broadband Router* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/bbfw/p2mp/index.htm

The fixed wireless multipoint system incorporates Vector Orthogonal Frequency Division Multiplexing (VOFDM), so it does not always depend on line-of-sight (LOS) deployment. With VOFDM, the system allows wireless operation in obstructed, non-line-of-sight (non-LOS) environments by taking advantage of multipath signals. This can be particularly useful in urban and suburban environments.

Wireless Network Module

The NM-WMDA wireless network module installs in the network module slot of a Cisco 2600 series router. Installing a wireless network module enables the Cisco 2600 series router to act as a subscriber unit (SU) in a point-to-multipoint wireless network. It is configured through the router's system console or via the CiscoView network management system. The network module provides the control and data interface between the Cisco 2600 series digital motherboard and the radio frequency (RF) subsystem in the wireless transverter. It also provides the up/down conversion from baseband to intermediate frequency (IF). One network module supports one or two wireless transverters (main and diversity).

Microcode software images ship in Flash memory along with the system software image. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface line cards.

It is possible to use a later version of microcode software than the one shipped with the Cisco IOS software from the factory. The microcode software in Flash memory is mapped to the line cards. Unless you fully understand how Cisco IOS software uses microcode software, it is important to keep the factory configuration.

CPMI CORREIOS
Fls. Nº 0486
Doc. 3690

The multipoint wireless modem card requires external microcode software. Information about this microcode software is available (with a Cisco.com login) at the following location:

http://www.cisco.com/cgi-bin/tablebuild.pl/rsu

For further information regarding the network module, refer to the *Cisco Network Modules Hardware Installation Guide* (for Cisco 2600 series routers) for detailed installation instructions, and the *Software Configuration Guide* (for Cisco 2600 series routers) for an overview of network module configuration procedures and information on configuring specific network modules.

New Software Features Supported in Cisco IOS Release 12.3

The following are new software features supported in Cisco IOS Release 12.3:

- AAA-PPP-VPDN Non-Blocking, page 143
- Accounting of VPDN Disconnect Cause, page 143
- ACL Default Direction, page 143
- ADSL over ISDN, page 144
- Advanced Voice Busyout, page 144
- Analog DID (Direct Inward Dial), page 144
- Asynchronous Serial Traffic Over User Datagram Protocol (UDP), page 144
- ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping, page 144
- ATM Service Level Monitoring (SLM), page 145
- ATM Subinterface MIB/Traps, page 145
- Automatic Bandwidth Adjustment for MPLS Traffic Engineering Tunnels, page 145
- Automatic Protection Switching (APS), page 146
- Barge-In and Busy Line Verify Operator Services, page 146
- BGP Link Bandwidth, page 146
- BRI QSIG Protocol, page 146
- Call Admission Control Based on CPU Utilization, page 147
- Call Admission Control for H.323 VoIP Gateways, page 147
- CDP and ODR Support for ATM PVCs, page 147
- CEF and Distributed CEF Switching for IPv6, page 148
- CEF on Multipoint GRE Tunnels, page 148
- Certificate Autoenrollment, page 148
- Certificate Enrollment Enhancements, page 148
- Circuit Interface Identification Persistence for SNMP, page 149
- Cisco Discovery Protocol (CDP)—IPv6 Address Family Support for Neighbor Information, page 149
- Cisco Gateway Management Agent, page 149
- Cisco IOS Firewall Stateful Inspection of ICMP, page 149
- Cisco IOS Firewall Support for SIP, page 149
- Cisco IOS Server Load Balancing, page 149

CPMI - CORREIOS
Fls. Nº 0487
3690
Doc.

- Cisco Mobile Networks—Dynamic Network Support, page 149
- Cisco Quality of Service Device Manager 2.0 Support for Cisco 1700 Series Routers, page 150
- Cisco Service Assurance Agent Support for the Cisco 820 Series and SOHO 70 Series, page 150
- Cisco VCWare Version Checker, page 150
- CISCO-BULK-FILE-MIB Enhancements, page 150
- CISCO-SIP-UA-MIB Enhancements Providing Functional Parity to SIP related CLI, page 151
- Class-Based Weighted Fair Queueing (CBWFQ), page 151
- CNS Agents SSL Security, page 151
- CNS Configuration Agent, page 151
- CNS Event Agent, page 151
- Committed Access Rate (CAR), page 152
- Connection-Oriented Media (Comedia) Enhancements for SIP, page 152
- Crashinfo Support for Cisco 3600 Series, page 152
- Default VPDN Group Template, page 152
- DF Bit Override Functionality with IPSec Tunnels, page 152
- DFP Support in DistributedDirector, page 152
- DHCP Client on WAN Interfaces, page 153
- DHCP Client—Dynamic Subnet Allocation API, page 153
- DHCP Relay Agent Support for Unnumbered Interfaces, page 153
- DHCP Server Import All Enhancement, page 153
- DHCP Server—On-Demand Address Pool Manager, page 153
- DHCP Server—Option to Ignore All BOOTP Requests, page 154
- Dialer CEF, page 154
- Dialer Watch Connect Delay, page 154
- Disabling V.110 Padding, page 154
- Distributed IPv6 for Cisco IOS Software, page 154
- Distributed Management Event MIB Conformance to RFC 2981, page 154
- DLR Enhancements: PGM RFC-3208 Compliance, page 154
- DLSw+ Enhanced Load Balancing, page 155
- DLSw+ Peer Group Clusters, page 155
- DNS Client AAAA Record Lookups over IPv6, page 155
- DNS Server Support for NS Records, page 155
- Dual Serial Line Management to Interface Lucent 5ESS, page 155
- E1 R2 Signaling, page 155
- Easy VPN Server, page 156
- Encrypted Vendor-Specific Attributes, page 156
- Enhanced Password Security, page 156
- Enhanced Test Command, page 156

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0488
Doc 3690

- Enhanced VoiceXML Diagnostics, page 157
- Enhancements for the Cisco VG200 Voice Gateway, page 157
- Update to the Enhancements for the Cisco Voice Gateway 200, page 157
- Event Tracer, page 158
- Fax and Modem Pass-Through over VoIP, page 158
- Fax Detection for VoiceXML, page 158
- File System Check and Repair for PCMCIA ATA Disks, page 159
- Firewall Authentication Proxy, page 159
- Firewall Feature Set, page 159
- Firewall Feature Set for Cisco 820 Series Routers, page 160
- Four SS7 Link Support on the Cisco Signaling Link Terminal, page 160
- Frame Relay Discard Eligibility Bit Setting, page 160
- Frame Relay PVC Bundles with IP and MPLS QoS Support, page 161
- Frame Relay Queueing and Fragmentation at the Interface, page 161
- Functionality Changed for the tunnel mpls traffic-eng autoroute metric Command, page 161
- G.SHDSL Symmetric DSL Support, page 161
- Gatekeeper-to-Gatekeeper Authentication, page 161
- Generic Routing Encapsulation (GRE) Tunnel Keepalive, page 162
- GKTMP Security Token Enhancement, page 162
- Global Modem Counters, page 162
- H.323 Call Redirection Enhancements, page 162
- H.323 Dual Tone Multifrequency Relay Using Named Telephone Events, page 162
- H.323 Redundant Zone Support, page 163
- H.323 Support for Virtual Interfaces, page 163
- H.323 Version 2 Phase 2, page 163
- High-Performance Gatekeeper, page 164
- HTTP 1.1 Client, page 164
- iBGP Multipath Load Sharing, page 164
- ICMP ECHO-Based RTT Probing by DRP Agents, page 164
- IGMP MIB Support Enhancements for SNMP, page 165
- IKE—Initiate Aggressive Mode, page 165
- Implementing OSPF for IPv6, page 165
- Integrated IS-IS Multi-Topology Support for IPv6, page 165
- Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media, page 165
- Integrated IS-IS Support for IPv6, page 166
- Interactive Voice Response Version 2.0 on Cisco VoIP Gateways, page 166
- Interactive Voice Response Version 2.0 on VoIP Gateways, page 167
- Interface Alias Long Name Support, page 167

RQS nº 03/2003 - CN
CPMI - CORREIOS
0489
Fls. Nº
3690
Doc.

- Interface Index Display, page 167
- Interim Local Management Interface (ILMI), page 167
- Interim Update at Call Connect, page 167
- Interim-Interswitch Signaling Protocol (IISP), page 168
- Interworking Signaling Enhancements for H.323 and SIP VoIP, page 168
- IP Header Compression Enhancement—PPPoATM and PPPoFR Support, page 168
- IP Multicast MIB Enhancements, page 168
- IP-FORWARDING-TABLE-MIB, page 168
- IPMROUTE-STD-MIB, page 168
- IPSec and 3DES Feature Set for Cisco 820 Series Routers, page 169
- Triple Data Encryption Standard Feature Set for Cisco 820 Series Routers, page 169
- IRR Triggers for GKTMP, page 169
- ISDN and V.120 Support for NextPort DSPs, page 169
- ISDN Progress Indicator Support for SIP Using 183 Session Progress, page 170
- ISIS: Allows BGP to Control the Configuration of the Overload Bit, page 170
- IVR: Enhanced Multilanguage Support, page 170
- Low Latency Queueing, page 170
- Low Latency Queueing with Priority Percentage Support, page 170
- LZ Software with Hardware Encryption, page 171
- MD5 File Validation, page 171
- Media Forking, page 171
- Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay, page 172
- MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles, page 172
- MGCP Basic CLASS and Operator Services, page 172
- MGCP CAS PBX and AAL2 PVC with Basic CLASS and Operator Services, page 173
- MGCP Generic Configuration Support for Call Manager (IP-PBX), page 174
- MGCP Line Package Enhancements for Loop Current Feed Open (LCFO), page 174
- MGCP PRI Backhaul and T1-CAS Support for Call Manager (IP-PBX), page 174
- MGCP Voice on Cisco AS5850 Universal Gateway, page 174
- MGCP VoIP Call Admission Control, page 175
- MGCP VoIP Signaling for 1750 Series, page 176
- Mobile IP —IPSec for Home Agent to Foreign Agent Tunnel, page 176
- Mobile IP MIB Support for SNMP, page 176
- Mobile IP—Fastswitching Support on Foreign Agent, page 176
- Mobile IP—Generic NAI Support and Home Address Allocation, page 176
- Mobile IP—MIB Support for NAI and HA Redundancy, page 177
- Mobile IP—Private Addressing Support, page 177

CPMI - CORREIOS
0490
Fls Nº
3690

- Mobile Networks, page 177
- Mobile Networks MIB Support, page 178
- Modem Script and System Script Support in Large-Scale Dial-Out, page 178
- MPLS Over ATM: Virtual Circuit (VC) Merge, page 178
- MPLS VPN ID, page 179
- Multicast Music on Hold Support for Call Manager (IP-PBX), page 179
- Multiple RSA Keypair Support, page 180
- NAT MIB (Read-Only), page 180
- NAT Protocol Translation, page 180
- NAT Support of H.323 RAS, page 180
- NAT-Support of H.323 v2 Call Signaling, page 180
- NetFlow Multiple Export Destinations, page 181
- NetFlow ToS-Based Router Aggregation, page 181
- NetWare Link Services Protocol (NLSP), page 181
- Network Access Server (NAS) Package for MGCP, page 181
- No Service Password-Recovery, page 181
- Nonblocking Gatekeeper AAA Interface, page 181
- OSPF Sham-Link Support for MPLS VPN, page 181
- Particle Drivers, page 182
- PIM MIB Extension for IP Multicast, page 182
- PIM Multicast Scalability, page 182
- Plain NFAS Support on NM-HDV, page 182
- PPPoE Connection Throttling, page 183
- PPPoE MTU Adjustment, page 183
- PPPoE over Gigabit Ethernet, page 183
- Preauthentication with ISDN PRI and Channel-Associated Signaling Enhancements, page 183
- PRI QSIG Protocol, page 183
- PSTN Fallback, page 183
- RADIUS Attribute 52 and Attribute 53 Gigaword Support, page 184
- RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements, page 184
- RADIUS Attribute 77 for DSL, page 184
- RADIUS Number Translation VSAs for VoIP, page 185
- RADIUS Route Download, page 185
- Reverse Path Forwarding - Source Exists Only, page 185
- Rotating Through Dial Strings, page 185
- RPR+ (Route Processor Redundancy Plus) on Cisco 7500 Series Routers, page 185
- RSVP Support for Low Latency Queueing, page 185
- Secure Shell (SSH) Support over IPv6, page 186

RQS nº 03/2005 - CN
CPMI - CORREIOS
0491
Fls - Nº
3690
Doc.

- Secure Shell (SSH) Version 1 Server Support, page 186
- SIP Diversion Header Implementation for Redirecting Number, page 186
- SIP Gateway Compliance to RFC2543-bis-04, page 187
- SIP Gateway Support for Third-Party Call Control, page 187
- SIP Gateway Support of RSVP and TEL URL, page 187
- SIP Intra-gateway Hairpinning, page 187
- SIP INVITE Request with Malformed Via Header, page 188
- SIP Multiple 18x Responses, page 188
- SIP T.37 Store and Forward Fax, page 188
- SIP T.38 Fax Relay, page 188
- SIP User Agent MIB, page 188
- SIP—Configurable PSTN Cause Code Mapping, page 188
- SIP—DNS SRV RFC2782 Compliance, page 189
- SIP—Session Initiation Protocol for VoIP, page 189
- SIP—Session Initiation Protocol for VoIP Enhancements, page 189
- SLT Dual Ethernet, page 190
- SLT G.732 Support, page 190
- SNMP IF-MIB Support for VLAN (ISL, 802.1Q) Subinterfaces, page 190
- SNMP Support over VPN, page 191
- SNMPv3 Community MIB Support, page 191
- Speech Recognition and Synthesis for Voice Applications, page 193
- Static Cache Entry for IPv6 Neighbor Discovery, page 193
- Supplementary Telephone Services for the Euro-ISDN Switch, page 193
- T.37 for Cisco 7200, page 194
- T.38 Fax Relay for VoIP H.323, page 194
- T1 Channel Associated Signaling (CAS), page 194
- TCL IVR 2.0 Call Initiation and Callback, page 194
- TCL IVR disconnect cause-code Manipulation, page 195
- TCL-Enabled Signaling Parameter Mapping, page 195
- TCP Window Scaling, page 195
- Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series Routers, page 195
- TX Ring Adjustment, page 195
- Using 31-Bit Prefixes on IPv4 Point-to-Point Links, page 195
- Virtual Circuit (VC) Merge, page 195
- VoAAL2 Profile 9 Support for BLES Interoperability, page 196
- Voice Application Access To SS7 Signaling, page 196
- Voice over IP Q.SIG Network Transparency, page 196
- VoiceXML For Cisco IOS, page 197

14301
RQS nº 03/2005 - CN
CPMI - CORREIOS
0492
Fls Nº
3690
Doc.

- VoiceXML Media Volume and Rate Controls, page 197
- VoiceXML SS7 ISUP Session Variables, page 197
- VoiceXML Transfer Enhancements, page 197
- VoiceXML Voice Store and Forward, page 197
- VoIP Call Admission Control Using RSVP, page 197
- VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP, page 198
- VRRP Support, page 198
- WRED Enhancement—Explicit Congestion Notification (ECN), page 198
- X.25 Over TCP Profiles, page 199
- X.25 Record Boundary Preservation for Data Communications Networks, page 199

AAA-PPP-VPDN Non-Blocking

Previously, Cisco IOS software created a statically configurable number of processes to authenticate calls. Each of these processes would handle a single call, but in some situations the limited number of processes could not keep up with the incoming call rate. This resulted in some calls timing out. The AAA-PPP-VPDN Non-Blocking feature changes the software architecture such that the number of processes will not limit the rate of call handling.

Accounting of VPDN Disconnect Cause

In the past, whenever a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) session fails or disconnects, the network access server (NAS) and Home GateWay (HGW) report a very generic disconnect-cause code, such as "LOST CARRIER". These generic codes do not provide enough detailed information for accounting and debugging purposes, creating a need for disconnect-cause codes that provide more detailed information. The Accounting of VPDN Disconnect Cause feature adds eight new disconnect-cause codes. These eight disconnect-cause codes describe the status of Virtual Private Dialup Network (VPDN) failures and disconnects more specifically than existing generic disconnect-cause codes. These new disconnect-cause codes can be found in the *Cisco IOS Security Configuration Guide*, Release 12.2, located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fappendx/fradattr/scfrdat3.htm

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm

ACL Default Direction

The ACL Default Direction feature allows you to change the filter direction (where filter direction is not specified) to inbound packets only; that is, you can configure your server to filter packets that are coming toward the network.

This feature introduces the **radius-server attribute 11 direction default** command, which allows you to change the default direction of filters for your access control lists (ACL) via RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router, thereby reducing resource consumption—rather than the outbound default direction, which waits until the traffic is about to leave the network before filtering. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0493
3690
Doc.

ADSL over ISDN

Cisco 826 routers connect corporate telecommuters and small offices via Internet service providers (ISPs) over asymmetric digital subscriber lines (ADSLs) to corporate LANs and the Internet. The router can provide bridging and multiprotocol routing between LAN and WAN ports. Cisco 826 routers provide connectivity to an ISDN network through an ADSL port.

Advanced Voice Busyout

The local voice busyout feature provides a way to busy out a voice port or DS-0 group (time slot) if a state change is detected in a monitored network interface (or interfaces). When a monitored interface changes to a specified state—to out-of-service or in-service—the voice port presents a seized/busyout condition to the attached PBX or other customer premises equipment (CPE). The PBX or other CPE can then attempt to select an alternate route.

Advanced Voice Busyout adds the following functionality to the local voice busyout feature:

- For Voice over IP (VoIP), monitoring of links to remote, IP-addressable interfaces by use of service assurance agent (SAA).
- Configuration by voice class to simplify and speed up the configuration of voice busyout on multiple voice ports.

Using the Advanced Voice Busyout feature you can perform the following tasks:

- Configure individual voice ports to enter the busyout state if an SAA probe signal returned from a remote, IP-addressable interface detects loss of IP connectivity by crossing a specified delay or loss threshold.
- Define voice classes with specified busyout conditions, and assign a particular voice class to any number of voice ports.
- SAA probe monitoring of remote interfaces is intended for use with VoIP networks, although it can also be used with Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_cacbo.htm

Analog DID (Direct Inward Dial)

Analog Direct Inward Dial (DID) is now supported on Cisco 1700 series routers.

Asynchronous Serial Traffic Over User Datagram Protocol (UDP)

The Asynchronous Serial Traffic Over User Datagram Protocol (UDP) feature provides the ability to encapsulate asynchronous data into UDP packets, and then unreliably transmit this data without needing to establish a connection with a receiving device.

You load the data you want to transmit through an asynchronous port, and then transmit it, optionally, as a multicast or a broadcast. The receiving device(s) can then receive the data whenever it wants. If the receiver ends reception, the transmission is unaffected.

This process is referred to as UDP Telnet (UDPTN), although it does not—and cannot—use the Telnet protocol. UDPTN is similar to Telnet in that both are used to transmit data, but UDPTN is unique in that it does not require that a connection be established with a receiving device.

ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping

In a digital subscriber line (DSL) environment, many applications require the configuration of a large number of ATM permanent virtual circuits (PVCs). The ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping feature enables you to group a number of PVCs into a PVC *range* in order to configure them all at once.

CORREIOS
Fls Nº 0494
Doc 3690

For applications that use multipoint subinterfaces, such as PPP over Ethernet and PPP over ATM, the PVC range is on a single multipoint subinterface. For applications that use point-to-point subinterfaces, such as routed bridge encapsulation (RBE), a point-to-point subinterface is created for each PVC in the range.

A PVC range is defined by two VPI-VCI pairs. The two virtual path identifiers (VPIs) define a VPI range, and the two virtual channel identifiers (VCIs) define a VCI range. The number of PVCs in the PVC range equals the number of VPIs in the VPI range multiplied by the number of VCIs in the VCI range.

Once the PVC range is defined, you can configure the range by using the existing interface-ATM-VC configuration commands that are also supported in ATM PVC range configuration mode. The **shutdown** ATM PVC range configuration mode command can be used to deactivate the range without deleting the configuration.

The ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping feature also introduces the **pvc-in-range** command, which allows you to explicitly configure an individual PVC within the defined range of PVCs on a multipoint subinterface. The **shutdown** ATM PVC-in-range configuration mode command allows you to deactivate an individual PVC within a range.

Note You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All of the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtatmpvr.htm

ATM Service Level Monitoring (SLM)

The Cisco Service Assurance Agent (SA Agent) is an embedded performance monitoring utility in Cisco IOS software. The ATM Service Level Monitoring (SLM) feature expands the capabilities of the SA Agent to provide detailed monitoring statistics for your ATM network. Monitoring service levels for ATM connections allows service providers to ensure that their networks are meeting or exceeding the performance outlined in service level agreements (SLAs).

The ATM Service Level Monitoring feature can also be used with Cisco Networking Services (CNS). A device running CNS, such as the IE2100, can be used to retrieve the ATM performance statistics generated by the SA Agent. Additionally, these results can be passed to other devices running third-party monitoring software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftatmslm.htm

ATM Subinterface MIB/Traps

This feature adds support for the monitoring of ATM and Frame Relay (FR) subinterface status using SNMP. New CLI commands allow the enabling or disabling of ATM and Frame Relay notifications (traps and informs), and provide an option for limiting the rate of notifications sent ("trap throttling").

Automatic Bandwidth Adjustment for MPLS Traffic Engineering Tunnels

Traffic engineering automatic bandwidth adjustment provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically (for example, once per day) adjusts the tunnel's allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

Fls. Nº 0495
Doc. 3690

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

There are three new commands:

- **clear mpls traffic-eng auto-bw timers**: Reinitializes the automatic bandwidth feature.
- **mpls traffic-eng auto-bw timers**: Enables automatic bandwidth adjustment for a platform and starts output rate sampling for tunnels configured for automatic bandwidth adjustment.
- **tunnel mpls traffic-eng auto-bw**: Configures a tunnel for automatic bandwidth adjustment and controls the manner in which the bandwidth for a tunnel is adjusted.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbwadjm.htm.

Automatic Protection Switching (APS)

This feature allows switchover of Packet-over-SONET (POS) circuits in the event of circuit failure and is often required when connecting SONET equipment to telco equipment.

Barge-In and Busy Line Verify Operator Services

The Barge-In and Busy Line Verify Operator Services feature enhances Simple Gateway Control Protocol (SGCP)/Media Gateway Control Protocol (MGCP) gateway conferencing capabilities to support the Busy Line Verification/Operator Interrupt (BLV/OI) feature. The Busy Line Verification feature permits an operator to establish a connection to a customer's line to verify a busy condition for a calling party. The Operator Interrupt feature allows the operator to speak to the customer and to connect the calling party and customer, if appropriate. These enhancements support other call flows such as call pickup with barge-in that require the ability to conference a second call into an existing two-party call without intervention by parties in the existing call. No explicit configuration is required to enable this feature.

The MGCP Basic CLASS and Operator Services feature introduced conferencing to support three-way calling on SGCP and MGCP gateways. It is described in MGCP Basic CLASS and Operator Services at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm

BGP Link Bandwidth

The Border Gateway Protocol (BGP) Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. The BGP Link Bandwidth feature is supported by the internal BGP (iBGP) and external BGP (eBGP) multipath features. The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. The link bandwidth extended community attribute may be propagated to all iBGP peers and used with the BGP multipath features to configure unequal cost load balancing. When a router receives a route from a directly connected external neighbor and advertises this route to iBGP neighbors, the router may advertise the bandwidth of that link.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftbgplb.htm

BRI QSIG Protocol

BRI QSIG is the QSIG support over BRI interface. QSIG protocol support allows Cisco voice gateways to connect PBXs, key telephone systems (KTS), and central office switches that communicate by using the QSIG protocol.

Call Admission Control Based on CPU Utilization

The Preauthentication with ISDN PRI feature permits the Cisco AS5300 and AS5800 universal access servers to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system CPU load level value. This feature helps ensure the quality of service (QoS) of existing calls and

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0496
Doc 3690

reliability of system processes by preventing system overload that is caused by excessive incoming calls. The feature rejects new digital calls (PRI, channel-associated signaling [CAS], and ISDN), with minor disruption to system users.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/dt61294.htm

Call Admission Control for H.323 VoIP Gateways

Before the call admission control feature, gateways did not have a mechanism to gracefully prevent calls from entering when certain resources were not available to process the call. This causes the new call to fail with unreported behavior, and could potentially cause the calls that are in progress to have quality related problems.

This feature set provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, and call volume, and interface resources such as call volume.

If system resources are not available to admit the call, two kinds of actions are provided: system denial (which busyouts all of T1 or E1) or per call denial (which disconnects, hairpins, or plays a message or tone). If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

This feature is supported on the Cisco 2600 and Cisco 3600 routers, Cisco MC3810 multiservice concentrators, and the Cisco IAD2420 platform.

CDP and ODR Support for ATM PVCs

This feature introduces support for the Cisco Discovery Protocol (CDP) over ATM point-to-point permanent virtual circuits (PVCs). Prior to this release, CDP discovery messages were not supported over ATM interfaces.

CDP is a Cisco proprietary device discovery protocol. Each Cisco device periodically sends messages to a multicast address. These messages advertise information about that device, such as the system ID (name), capabilities, Cisco IOS software version, and the network address of the connected interface. This information will be picked up by any neighboring Cisco devices on the same medium, which are listening for CDP advertisements. The information learned about neighboring devices is available through the Cisco IOS CLI **show cdp** commands and through SNMP monitoring using the CDP MIB.

This feature also adds support for On-Demand Routing (ODR) over ATM PVCs. ODR uses CDP to propagate IP address information in hub-and-spoke topologies. When ODR is enabled, spoke routers automatically advertise their subnets using CDP.

CDP is disabled by default for ATM PVC interfaces. To enable CDP, use the **cdp run** global configuration mode command and the **cdp enable** interface configuration mode command on both ends of the PVC. To enable ODR, use the **router odr** global configuration mode command on the hub router and turn off any dynamic routing protocols in the spoke routers.

For details on configuring CDP, refer to the following documentation:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf015.htm

For details on configuring ODR, refer to the following documentation:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfodr.htm

CEF and Distributed CEF Switching for IPv6

Cisco Express Forwarding for IPv6 (CEFv6) is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed CEF for IPv6 (dCEFv6) performs the same functions as CEFv6 but for distributed architecture platforms such as the Cisco 12000 series Internet routers and the Cisco 7500 series routers. dCEFv6 and CEFv6 function the same and offer the same benefits as dCEFv4

EOS Nº 03/05 - CN
CPMI - CORREIOS
0197
Fls. Nº
Doc. 3690

and CEFv4—network entries that are added, removed, or modified in the IPv6 Routing Information Base (RIB), as dictated by the routing protocols in use, are reflected in the Forwarding Information Bases (FIBs), and the IPv6 adjacency tables maintain Layer 2 next-hop addresses for all entries in each FIB.

CEFv6 was introduced in Cisco IOS Release 12.2(13)T for nondistributed architecture platforms, such as the Cisco 7200 series routers. dCEFv6 was introduced in Cisco IOS Release 12.0(21)ST for the Cisco 12000 series Internet routers, and was then integrated into Cisco IOS Release 12.2(13)T and later releases for other distributed architecture platforms, such as the Cisco 7500 series routers.

In Cisco IOS Release 12.0(21)ST, dCEFv6 included support for IPv6 addresses and prefixes. In Cisco IOS Release 12.2(13)T or later releases, dCEFv6 and CEFv6 were enhanced to include support for separate FIBs for IPv6 global, site-local, and link-local addresses.

CEF on Multipoint GRE Tunnels

The CEF on Multipoint GRE Tunnels feature enables Cisco Express Forwarding (CEF) switching of IP traffic to and from multipoint generic routing encapsulation (GRE) tunnels. Tunnel traffic can be forwarded to a prefix through a tunnel destination when both the prefix and the tunnel destination are specified by the application.

C..icate Autoenrollment

The Certificate Autoenrollment feature allows you to configure your router to automatically request a certificate from the certification authority (CA) that is using the parameters in the configuration. Thus, operator convention is no longer required at the time the enrollment request is sent to the CA server.

Automatic enrollment will be performed on startup for any trustpoint CA that is configured and does not have a valid certificate. When the certificate—which is issued by a trustpoint CA that has been configured for autoenrollment—expires, a new certificate is requested. Although this feature does not provide seamless certificate renewal, it does provide unattended recovery from expiration.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftautoen.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 platforms.

Certificate Enrollment Enhancements

The Certificate Enrollment Enhancements feature introduces five new subcommands to the **crypto ca trustpoint** command—**ip-address** (ca-trustpoint), **password** (ca-trustpoint), **serial-number**, **subject-name**, and **usage**. These commands provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts. (However, the prompting behavior remains the default if this feature is not enabled.) Thus, users can preload all necessary information into the configuration, allowing each router to obtain its certificate automatically when it is booted.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftenrol2.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 platforms.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0498
3690
Doc.

Circuit Interface Identification Persistence for SNMP

The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object (cciDescr) which can be used to identify individual circuit-based interfaces for SNMP monitoring. The Circuit Interface Identification Persistence for SNMP feature maintains this user-defined name of the circuit across reboots, allowing the consistent identification of circuit interfaces. Circuit Interface Identification Persistence is enabled using the **snmp mib persist circuit** global configuration command.

Note This feature was originally introduced in Cisco IOS Release 12.1(4)T. This release is porting the feature into the Cisco AS5300 platform.

Cisco Discovery Protocol (CDP)—IPv6 Address Family Support for Neighbor Information

The CDP IPv6 Address Family Support for Neighbor Information feature adds the ability to transfer IPv6 addressing information between two Cisco devices using Cisco Discovery Protocol (CDP). CDP in IPv6 functions the same as and offers the same benefits as CDP in IPv4. IPv6 enhancements to CDP allow CDP to exchange IPv6 and neighbor addressing information. IPv6 CDP provides IPv6 information to network management products and provides troubleshooting tools.

Cisco Gateway Management Agent

The Cisco Gateway Management Agent (CGMA) feature provides an eXtensible Markup Language (XML) interface to support real-time management of a Cisco IOS gateway (GW). Currently, GWs provide statistics using Simple Network Management Protocol (SNMP) and do not support real-time polling. The CGMA feature allows GWs to communicate with third-party management applications using XML over TCP/IP.

Cisco IOS Firewall Stateful Inspection of ICMP

The Cisco IOS Firewall Stateful Inspection of ICMP feature addresses the limitation of qualifying Internet Control Management Protocol (ICMP) messages into either a malicious or benign category by allowing the Cisco IOS firewall to use stateful inspection to "trust" ICMP messages that are generated within a private network and to permit the associated ICMP replies. Thus, network administrators can debug network issues without needing to block ICMP messages from entering the network because of possible intruders.

Cisco IOS Firewall Support for SIP

The Cisco IOS Firewall Support for SIP feature integrates Cisco IOS firewalls, the Voice over IP (VoIP) protocol, and Session Initiation Protocol (SIP) within a Cisco IOS based platform, enabling better network convergence.

Cisco IOS Server Load Balancing

The IOS SLB feature is a Cisco IOS-based solution that provides IP server load balancing. Using the IOS SLB feature, the network administrator defines a virtual server that represents a group of real servers in a cluster of network servers known as a server farm. In this environment the clients are configured to connect to the IP address of the virtual server. The virtual server IP address is configured as a loopback address, or secondary IP address, on each of the real servers. When a client initiates a connection to the virtual server, the IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/iosslb5t.htm

Cisco Mobile Networks—Dynamic Network Support

The Cisco Mobile Networks feature enables a mobile router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this mobile router. Previously, this feature was a static network implementation that supported stub routers only.

RQS nº 03/2005 - CN
CPMI
CORREIOS
Fls. Nº 0439
Doc. 3690

Cisco IOS Release 12.2(13)T introduces dynamic network support, which means that the mobile router dynamically registers its mobile networks to the home agent, which reduces the amount of configuration required at the home agent. For example, if a home agent supports 2000 mobile routers, the home agent does not need 2000 configurations but only a range of home IP addresses to use for the mobile routers.This registration results in minimal configuration on the home agent making administration and set up easier.

Cisco Quality of Service Device Manager 2.0 Support for Cisco 1700 Series Routers

QDM is now supported on Cisco 1700 series routers.

Cisco Quality of Service Device Manager (QDM) is a web-based Java application with which users can configure and monitor advanced IP-based Quality of Service (QoS) functionality within Cisco routers using a graphical user interface (GUI).

QDM 2.0 is available as a separate product download and is free of charge. If you would like to install or reinstall QDM, refer to the Release and Installation Notes for Cisco Quality of Service Device Manager 2.0 on Cisco.com and the Documentation CD-ROM for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qdm/qdmrn20.htm

Cisco Service Assurance Agent Support for the Cisco 820 Series and SOHO 70 Series

For information on configuration for the Cisco Service Assurance Agent, refer to the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf017.htm

The Cisco 820 series and SOHO 70 series do not currently support the Cisco Service Assurance Agent Application Performance Monitor (APM) feature.

Cisco VCWare Version Checker

The Cisco VCWare Version Checker feature adds Cisco VCWare version checker warning output at bootup and when you use the **show vfc version vcware** and **show vfc version dspware** commands.

This new version checker feature detects possible mismatches between Cisco IOS software and Cisco VCWare and DSPWare. If a software mismatch is found, a compatibility mismatch warning is output at bootup and when the **show vfc version** commands are used. If no mismatch is found, there is no advisory output. Because the new information is advisory only, there is no action taken whether the software is compatible or incompatible.

This feature applies only to the Cisco AS5300. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftvdspck.htm

CISCO-BULK-FILE-MIB Enhancements

The Cisco Bulk File Creation MIB (CISCO-BULK-FILE-MIB.my) is a MIB module for creating and deleting bulk files of SNMP data for file transfer. The CISCO-BULK-FILE-MIB Enhancements feature enhances the Cisco Bulk File Creation MIB to support selective-row-transfer and notification-on-file-creation. Prior to this enhancement, when the MIB was used to dump large tables (for example, the ccHistoryTable), much of the data transfer consisted of duplicated data. This feature allows the SNMP manager to specify a starting row in the SNMP Get request.

This feature also introduces a notification that can be sent when file creation is complete or when there is an error during file creation. Specifically, this feature modifies the CISCO-BULK-FILE-MIB by introducing four new MIB objects (cbfDefineFileNotifyOnCompletion, cbfDefineObjectTableInstance, cbfDefineObjectNumEntries, cbfDefineObjectLastPolledInst) and a new notification object (cbfDefineFileCompletion). For details, refer to the CISCO-BULK-FILE-MIB.my file, available through Cisco.com MIB FTP site at the following location:

ftp://ftp.cisco.com/pub/mibs/v2/CISCO-BULK-FILE-MIB.my

ECT-BRASIL/BR - CN
CORREIOS
0500
Fls. Nº
Doc. 3690

CISCO-SIP-UA-MIB Enhancements Providing Functional Parity to SIP related CLI

The CISCO-SIP-UA-MIB Enhancements Providing Functional Parity to session initiation protocol (SIP) related CLI feature has Simple Network Management Protocol (SNMP)/command-line interface (CLI) MIB enhancements to maintain parity with SIP features released to date.

No documentation work is required. The MIB is "self-documenting."

Class-Based Weighted Fair Queueing (CBWFQ)

Class-based weighted fair queueing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.

CNS Agents SSL Security

CNS Agents SSL Security is a Cisco IOS software feature that allows for the configuration of a secure connection between the CNS Agent, running on the Cisco IOS software-based device, and a CNS Server. Secure Socket Layer (SSL) encryption for CNS connections is enabled on the Cisco IOS device (CNS Agent) side using the **encrypt** keyword with the **cns config initial** or **cns config partial** global configuration mode commands.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

CNS Configuration Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Configuration Agent supports routing devices by providing:

- Initial configurations
- Incremental (partial) configurations
- Synchronized configuration updates

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ca.htm

Note This feature was originally introduced in Cisco IOS Release 12.1(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

CNS Event Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications, for example CNS Configuration Agent, to publish and subscribe to events on a CNS Event Bus. CNS Event Agent works in conjunction with CNS Configuration Agent.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ea.htm

ECT/EBT CORREIOS
Fls. Nº 0501
Doc 3690

14290

Note This feature was originally introduced in Cisco IOS Release 12.1(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Committed Access Rate (CAR)

Committed Access Rate (CAR) can rate limit traffic based on certain matching criteria, such as incoming interface, IP Precedence, or IP access list.

Connection-Oriented Media (Comedia) Enhancements for SIP

This feature provides the following functionality to symmetric Network Address Translation (NAT) traversal:

- Allows the Cisco gateway to check the media source of incoming Real-time Transport Protocol (RTP) packets.
- Allows the endpoint to advertise its presence inside or outside of NAT.

The new feature implements one of many possible SIP solutions to address problems with different NAT types and traversals.With the Connection-Oriented Media (Comedia) Enhancements for SIP feature, the gateway can open an RTP session with the remote end and then update or modify the existing RTP session's remote address and port (**raddr:rport**) with the source address and port of the actual media packet received after passing through NAT.

Crashinfo Support for Cisco 3600 Series

Crashinfo is a mechanism to reliably and quickly store useful information related to unexpected system shutdowns directly to a local flash card. This information can be retrieved after a system reload to aid in the analysis and resolution of a system error.

To enable this feature, use the **exception crashinfo file** *device:filename* in global configuration mode. Use the device and filename arguments to specify the flashcard and file to be used for storing the diagnostic information. To change the size of the crashinfo buffer, use the **exception crashinfo buffersize** command. The default buffer size is 32 kilobytes.

Default VPDN Group Template

The Default VPDN Group Template feature introduces the ability to configure global default values for virtual private dialup network (VPDN) parameters in a VPDN template. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups. Previously, the Cisco IOS software required that VPDN parameters be configured for each individual VPDN group if the system default values were not desired.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdevpdn.htm

DF Bit Override Functionality with IPSec Tunnels

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPSec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftdfipsc.htm

DFP Support in DistributedDirector

DistributedDirector can obtain load information from Cisco LocalDirector, Catalyst 4840g, and other clients using Dynamic Feedback Protocol (DFP). This protocol allows the user to configure the DistributedDirector to communicate with various DFP agents. The DistributedDirector tells the DFP agents how often they should report load information; then the DFP agent can tell the DistributedDirector which LocalDirector cluster to remove from providing service.

Refer to the following document for additional information:

ECT ROS nº 0502 CPMI CORREIOS
Fls. Nº
Doc. 3690

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/distrdir/dtdddfp.htm

DHCP Client on WAN Interfaces

The DHCP Client on WAN Interfaces feature extends the Dynamic Host Configuration Protocol (DHCP) to allow PPP over ATM (PPPoA) and certain ATM interfaces to acquire an IP address through DHCP. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as DNS server addresses, the DNS default domain name, and default route.

Previously, the **ip address dhcp** interface configuration command could only be used on Ethernet interfaces. This feature allows the **ip address dhcp** command to be used on WAN interfaces.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftwandhp.htm.

DHCP Client—Dynamic Subnet Allocation API

The DHCP Client–Dynamic Subnet Allocation API feature is an application program interface (API) that is called by the DHCP Server–On-Demand Address Pool Manager feature for obtaining a subnet or releasing a subnet to the source server via DHCP. This feature allows automated configuration of Layer 3 devices for simplified deployment.

DHCP Relay Agent Support for Unnumbered Interfaces

Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. Relay Agents receive Dynamic Host Configuration Protocol (DHCP) messages and then generate a new DHCP message to send out on another interface.

The Cisco IOS DHCP relay agent supports IP unnumbered interfaces. The DHCP relay agent automatically adds a static host route specifying the unnumbered interface as the outbound interface.

DHCP Server Import All Enhancement

When the import all DHCP pool configuration command is used, the DHCP Server Import All Enhancement feature allows options imported by one subsystem to coexist with options imported from another subsystem. When the session is terminated or the lease is released, the imported options are cleared from the DHCP server database.

DHCP Server—On-Demand Address Pool Manager

The DHCP Server–On-Demand Address Pool Manager is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. This feature supports address assignment using the Dynamic Host Configuration Protocol (DHCP) for customers using private addresses. Each on-demand address pool (ODAP) is configured and associated with a particular Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

When configured, the ODAP is populated with one or more subnets leased from a source server and is ready to serve address requests from DHCP clients or from PPP sessions. The source server can be a remote DHCP server or a RADIUS server (via AAA). Currently, only the Cisco Access Registrar RADIUS server supports ODAPs. Subnets can be added to the pool when a certain utilization level (high utilization mark) is achieved. When the utilization level falls below a certain level (low utilization mark), a subnet can be returned to the server from which it was originally leased.

This feature allows customers to optimize their use of IP addresses, thus conserving address space.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftondhcp.htm

CPMI - 0503
Fls Nº
Doc. 3690

DHCP Server—Option to Ignore All BOOTP Requests

The DHCP Server—Option to Ignore All BOOTP Requests feature introduces the following new global configuration command: **ip dhcp bootp ignore**. This command allows the Cisco IOS DHCP server to ignore received BOOTP requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdbootp.htm

Dialer CEF

The Dialer CEF feature introduces Cisco Express Forwarding (CEF) support for dialer interfaces. The Dialer CEF feature allows packets to be CEF switched across dialer interfaces rather than being low-end switched (LES) or fast switched. Compared to fast switching, CEF switching support improves switching performance by decreasing CPU utilization and lowering the packet loss rate. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdlrcef.htm

Dialer Watch Connect Delay

The Dialer Watch Connect Delay feature introduces the ability to configure a delay in bringing up a secondary link when a primary link that is monitored by Dialer Watch goes down and is removed from the routing table. Previously, the router would instantly dial a secondary route without allowing time for the primary route to come back up. When the Dialer Watch Connect Delay feature is configured, the router will check for availability of the primary link at the end of the specified delay time before dialing the secondary link.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdialwl.htm

Disabling V.110 Padding

In networks with devices such as terminal adapters (TAs) and global system for mobile communication (GSM) handsets that do not fully conform to the V.110 modem standard, you will need to disable V.110 padding. To disable the padded V.110 modem speed report required by the V.110 modem standard, use the **no isdn v110 padding** command in interface configuration mode.

Distributed IPv6 for Cisco IOS Software

This feature provides distributed CEF switching support for IPv6 on the Cisco 7500 platforms.

Distributed Management Event MIB Conformance to RFC 2981

Prior to Cisco IOS Release 12.2(4)T3, Event MIB support in Cisco IOS software was based on the IETF internet draft version. In Cisco IOS Release 12.2(4)T3, the Cisco implementation of the EVENT-MIB was updated to comply with the finalized version of the Event MIB, as defined in RFC 2981. For details, see RFC 2981, available through the IETF website at http://www.ietf.org.

DLR Enhancements: PGM RFC-3208 Compliance

In compliance with RFC 3208, the DLR Enhancements feature adds off-tree designated local repairer (DLR) support and redirecting poll response (POLR) capability for upstream DLRs to the Cisco implementation of Pragmatic General Multicast (PGM).

ROS nº 03/2005 - CN
CPMI - CORREIOS
0504
Fls. Nº
Doc. 3690

DLSw+ Enhanced Load Balancing

In a network with multiple capable paths, the Data Link Switch Plus (DLSw+) Load Balancing Enhancements feature improves traffic load balancing between peers by distributing new circuits based on existing loads and the desired ratio.

For each capable peer (peers that have the lowest or equal cost specified), the DLSw+ Load Balancing feature calculates the difference between the desired and the actual ratio of circuits being used on a peer. It detects the path that is underloaded in comparison to the other capable peers and assigns new circuits to that path until the desired ratio is achieved.

Note This feature was originally introduced in Cisco IOS Release 12.0(3)T. This release is porting the feature into the Cisco AS5350 platform.

DLSw+ Peer Group Clusters

The DLSw+ Peer Group Clusters feature reduces the explorer packet replication that typically occurs in a large Data Link Switch Plus (DLSw+) peer group design, where there are multiple routers connected to the same LAN.

The DLSw+ Peer Group Clusters feature associates DLSw+ peers (that are connected to the same LAN) into logical groups. Once the multiple peers are defined in the same peer group cluster, the DLSw+ Border Peer recognizes that it does not have to forward explorers to more than one member within the same peer group cluster.

Note This feature was originally introduced in Cisco IOS Release 12.0(3)T as DLSw+ Peer Clusters. This release is porting the feature into the Cisco AS5350 platform.

DNS Client AAAA Record Lookups over IPv6

The DNS Lookups over an IPv6 Transport feature adds support for IPv6 AAAA record types over an IPv6 transport in the Domain Name System (DNS) name-to-address and address-to-name lookup processes.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/index.htm

DNS Server Support for NS Records

DistributedDirector has improved server load-balancing capacity with the DNS Server Support for NS Records feature. This feature adds support for name server (NS) records to the Cisco IOS Domain Name System (DNS) server. With this feature, the DistributedDirector can distribute the server-selection process to multiple DistributedDirectors, improving overall server capacity.

Dual Serial Line Management to Interface Lucent 5ESS

This feature is a part of the Cisco IOS Telco Feature Set, a bundle of applications specific to the data communications network (DCN) environment. Specifically, this feature supports X.25-to-TCP protocol translation, and provides dual serial interfaces to preserve the redundancy and monitoring capability available from SCC0 and SCC1 links on a Lucent 5ESS switch in the DCN network.

E1 R2 Signaling

R2 signaling is an international signaling standard that is common to channelized E1 networks. The E1 R2 Signaling feature was introduced in Cisco IOS Release 11.3(2)T and is now supported on Cisco 1751 and Cisco 1760 platforms in Cisco IOS Release 12.2(15)T and Cisco IOS Release 12.3.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0505
3690

A client process, such as HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP), can now register with the tracking service, its interest in tracking a particular object, such as an interface or a route, and then be notified when the tracked object changes state. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/fthsrptk.htm

Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x software clients and Cisco VPN hardware clients. It allows a remote end user to communicate using IP Security (IPSec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunity.htm

Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature introduces support for the following three types of string vendor-specific attributes (VSAs):

- Tagged string VSA—To retrieve the right value for this VSA, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server will ignore the value and consider the Tag field to be a part of the attribute string field.
- Encrypted string VSA—This VSA has a Salt field that ensures the uniqueness of the encryption key that is used to encrypt each instance of the VSA. The first and most significant bit of the Salt field must be set to 1.
- Tagged and Encrypted string VSA—This VSA is similar to encrypted string VSAs *except* this VSA has an additional Tag field. If the Tag field is not within the valid range (0x01 0x01 through 0x1F), it is considered to be part of the Salt field.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftencvsa.htm

Enhanced Password Security

The Enhanced Password Security feature allows you to configure Message Digest 5 (MD5) encryption for username passwords. Before the introduction of this feature, there were two types of passwords associated with usernames: Type 0, which is a clear text password visible to any user who has access to privileged mode on the router, and type 7, which is a password with a weak, exclusive, or type encryption. Type 7 passwords can be retrieved from the encrypted text by using publicly available tools.

Use the **username secret** command to configure a username and an associated MD5-encrypted secret.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_md5.htm

Enhanced Test Command

The Enhanced Test Command feature introduces two new commands—**aaa user profile** and **aaa attribute**—that allow you to create a named user profile with calling line identification (CLID) or dialed number identification service (DNIS) attribute values, which can be associated with a **test aaa group** command.

Fls Nº 0506
3690

Use the **aaa attribute** command to add CLID or DNIS attribute values to a user profile, which is created by using the aaa user profile command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the test aaa group command), thereby providing the RADIUS server with access to CLID or DNIS attribute information for all incoming calls. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaaacmd.htm

Enhanced VoiceXML Diagnostics

With the Enhanced VoiceXML Diagnostics feature, debugging output can be filtered for all VoiceXML applications except the application named in the **debug condition application voice** command. When this command is configured, the gateway displays debugging messages only for the specified VoiceXML application when using the **debug vxml** and **debug http client** commands.

Refer to the following documents for additional information:

- Cisco IOS TCL and VoiceXML Application Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm

- Cisco VoiceXML Programmer's Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/vxmlprg/index.htm

Enhancements for the Cisco VG200 Voice Gateway

The Enhancements for the Cisco VG200 Voice Gateway feature provides the Cisco VG200 platform with increased voice gateway feature parity to the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series. This feature is also supported on the Cisco VG200XM platform upgrade. The Cisco VG200XM is new for Cisco IOS Release 12.2(11)T and is a more powerful version of the Cisco VG200, offering higher processing power and improved performance.

The Cisco VG200 platforms provide the following default memory options:

- CiscoVG200—8 MB of Flash, 64 MB of DRAM.
- Cisco CG200XM—16 MB of Flash, 64 MB of DRAM.

The Enhancements for the Cisco VG200 Voice Gateway feature includes the following features:

- FXO Answer and Disconnect supervision—Enables analog Foreign Exchange Office (FXO) ports to monitor call-progress tones and to monitor voice and fax transmissions returned from a PBX or from the Public Switched Telephone Network (PSTN).
- NM-HDV-1T1/E1-12—This digital voice card provides telephony interface signaling support, providing a lower density digital solution.
- Private-line automatic ringdown (PLAR)—Provides an off-premises extension (OPX) from a private PBX. Also provides dial tone from a remote PBX.
- Proprietary Transfer Code—Enables the Cisco VG200 (acting as a PSTN gateway with an Survivable Remote Site Telephony (SRST) or ITS device) to support Cisco proprietary call transfer from the SRST or ITS device back to the PSTN.

Update to the Enhancements for the Cisco Voice Gateway 200

The Enhancements for the Cisco Voice Gateway 200 (Cisco VG200) feature provides the Cisco VG200 platform (also called CAG-VG200) with increased voice gateway feature parity to the Cisco 2600, Cisco 3600, and Cisco 3700 platforms. This update provides additional feature functionality on the Cisco VG200 platform.

The Cisco VG200 platforms provide the following default memory options: CAG-VG200—16 MB of Flash, 64 MB of DRAM.

0507
3690

14284

Event Tracer

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, route processor switchover.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s18/evnttrcr.htm

Fax and Modem Pass-Through over VoIP

On detection of the fax or modem tone on an established VoIP call, the gateways switch into modem fax or pass-through mode: the voice codec and configuration is suspended and the pass-through parameters are loaded for the duration of the fax or modem session. This changes the bandwidth needed for the call to the equivalent of G.711.

With pass-through, the fax or modem traffic is carried between the two gateways in RTP packets, using an uncompressed format resembling the G.711 codec. Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, fax and modem pass-through remain susceptible to packet loss, jitter and latency in the IP network. The two endpoints must be clocked synchronously for this type of transport to work predictably.

The Fax and Modem Pass-Through feature is also known as Voice Band Data (VBD) by the International Telecommunication Union (ITU). VBD refers to the transport of fax or modem signals over a voice channel through a packet network with an encoding appropriate for fax or modem signals. The minimum set of coders for VBD mode is G.711 ulaw and alaw with VAD disabled. For modem transport, Echo cancellation is also be disabled.

Note The Fax and Modem Pass-Through over VoIP feature is also known under the feature title Modem Passthrough over Voice over IP.

Fax Detection for VoiceXML

With the Fax Detection for VoiceXML feature, when a VoiceXML fax detection application is configured on the gateway, callers can dial a single number for both voice and fax calls. The gateway automatically detects that a call is a fax transmission by listening for comfort noise generation (CNG), the distinctive fax "calling" tone. When configured for fax detection, the Cisco VoiceXML gateway continuously listens to incoming calls to determine which calls are voice or fax. The gateway then routes the calls to the appropriate application or media server.

Refer to the following documents for additional information:

- Cisco IOS TCL and VoiceXML Application Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm

- Cisco VoiceXML Programmer's Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/vxmlprg/index.htm

RCTS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0508
3690
Doc

File System Check and Repair for PCMCIA ATA Disks

This feature introduces a File-System-Check (fsck) utility in Cisco IOS software for FAT filesystems on PCMCIA disks. The utility performs functions such as checking the boot sector and partition table, checking file and directory structure, reclaiming unused disk space, and updating the FAT file structure. Prior to the introduction of this utility, corrupt files could not be removed from ATA disks using the Cisco IOS CLI. This utility is run using the **fsck** privileged EXEC mode command.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_fsck.htm

Firewall Authentication Proxy

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with the IP address of a user, or a single security policy had to be applied to an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and Cisco Secure VPN Client (VPN client) software.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdauthp.htm

Firewall Feature Set

The Cisco IOS Firewall feature set provides firewall-specific security features to the Cisco CVA122 Cable Voice Adapter. When this feature is enabled, the router acts as a buffer between the Internet and other public networks and the private network that is connected to the router. Security is provided by access lists, as well as by examining incoming traffic for suspicious activity.

The firewall-specific security features include the following:

- Authentication proxy services to intelligently apply specific security policies on a per-user basis without impacting performance.
- Checking packet headers and dropping suspicious packets to detect and prevent denial of service attacks, such as ICMP and UDP echo packet flooding, SYN packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Context-Based Access Control (CBAC) which gives internal-to-the-firewall users secure, per-application-based traffic control across the Internet/Intranet. This includes protection against Simple Mail Transfer Protocol (SMTP) attacks, one of the most common attacks against computers connected to the Internet.
- Dynamic port mapping to allow network applications with well-known port assignments to use customized port numbers. This mapping can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Intrusion Detection System (IDS) that recognizes the signatures of the most common attack profiles. When an intrusion is detected, IDS can perform a number of actions: send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection

14283
CORREIOS
0309
3690

- Java blocking to protect against destructive Java applets. Applets can be allowed only from known and trusted sources or blocked completely.
- Real-time and configurable alerts and audit trail capabilities to record and time-stamp source and destination hosts.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- User-configurable audit rules, real-time alerts, and audit-trail logs.

Firewall Feature Set for Cisco 820 Series Routers

The Cisco IOS Firewall feature set is available on the Cisco 820 series routers. This feature set provides the following capabilities:

- Context-Based Access Control (CBAC)
- Java blocking
- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The Cisco IOS Firewall Feature Set feature module provides several sample firewall configurations, including the following examples for small-office environments:

- IP network to Internet
- Remote office network to corporate office network

Four SS7 Link Support on the Cisco Signaling Link Terminal

The Four SS7 Link Support on the Cisco Signaling Link Terminal feature introduces support for up to four Cisco SS7 links on a new platform for the Cisco SLT, the Cisco 2651 Multiservice Access Router. All existing Cisco 2611-based Cisco SLT functionality is supported on the new platform, and both Cisco SLT platforms use the same Cisco IOS software image.

The Cisco 2651-based Cisco SLT supports up to four SS7 A-links and F-links, and each SS7 link can support up to 0.4 erlangs of signaling traffic during normal operation. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_4lnk.htm

Frame Relay Discard Eligibility Bit Setting

The Modular QoS CLI has been enhanced to include matching and marking based on the Frame Relay Discard Eligibility (DE) bit. Frame Relay DE bit Matching and Marking is documented as part of the Class-Based Marking feature module.

The DE bit in the address field of a Frame Relay frame is used as a method for prioritizing the discarding of frames in congested frame relay networks. The Frame Relay DE bit has only one bit and can therefore only have two settings, 0 or 1. If congestion occurs in a Frame Relay network, frames with the DE bit set at 1 are discarded before frames with the DE bit set at 0. Therefore, important traffic should have the DE bit set at 0 and less important traffic should be forwarded with the DE bit set at 1.

The default DE bit setting is 0. The Class-Based Packet Marking feature allows users to change the DE bit setting to 1 for various traffic, giving users the option of keeping the default value of 0 or changing the value to 1. Users can therefore use the Frame Relay DE bit marking to prioritize frames in a Frame Relay network.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0510
Fls Nº
Doc. 3690

- H.450.3 Call Deflection
- Translation of FXS Hookflash Relay
- H.235 Security
- Gatekeeper Transaction Message Protocol (GKTMP) and RAS Messages
- Gatekeeper and Alternate Endpoints
- Gatekeeper C Code Generic API for GKTMP in a UNIX Environment
- Gateway Support for Network-Based Billing Number

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/h323v2p2.htm

High-Performance Gatekeeper

The Cisco High-Performance Gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into the Cisco voice network solution portfolio. These H.323 standard-based features have carrier grade reliability and performance characteristics with a robust open application protocol interface to enable development of enhanced applications like voice VPNs and wholesale voice solutions.

This feature addresses the scalability, redundancy, and performance aspects of the gatekeeper as part of the Cisco Multimedia Conference Manager (MCM) to present a complete Cisco solution. The Cisco H.323 MCM provides the network administrator with the ability to identify H.323 traffic and to apply appropriate policies.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ft_0394.htm

HTTP 1.1 Client

This feature implements support for HTTP clients within Cisco IOS software compliant with the HTTP 1.1 standard (RFC 2616). The HTTP 1.1 Client allows the network device to contact a remote web server and obtain content or interact with remote applications. The HTTP 1.1 Client is enabled by default on supported platforms.

iBGP Multipath Load Sharing

When a Border Gateway Protocol (BGP) speaker router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP for the same destination, the router will choose one internal BGP path as the best path. The best path is then installed in the IP routing table of the router.

The Internal BGP Multipath Load Sharing feature enables the BGP speaker router to select multiple internal BGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bmls.htm

ICMP ECHO-Based RTT Probing by DRP Agents

DistributedDirector users can now control Director Response Protocol (DRP) agents to send both TCP and ICMP packets for round-trip time (RTT) measurement.The RTT measurement is used to dynamically direct Internet customers to the closest regional web proxy based on response time.

In the original implementation, some Internet DNS servers did not respond when the DRP agents sent them a query to measure the RTT.

ECT/ECT 002/2005 - CN
CPMI - CORREIOS
Fls Nº 0511
Doc 3690

This feature introduces the new **ip director drp rttprobe tcp | icmp** command that enables DistributedDirector to instruct a DRP agent to send ICMP-echo packets to measure the RTT.

When both ICMP and TCP are enabled, DistributedDirector will instruct DRP agents to send both TCP and ICMP packets for RTT probing. The returned RTT from a DRP agent will be the RTT collected from either the TCP or ICMP mechanism, which ever becomes available first.

IGMP MIB Support Enhancements for SNMP

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. The IGMP MIB describes objects that enable users to remotely monitor and configure IGMP using Simple Network Management Protocol (SNMP). It also allows users to remotely subscribe and unsubscribe from multicast groups. The IGMP MIB Support Enhancements for SNMP feature adds full support of RFC 2933 (Internet Group Management Protocol MIB) in Cisco IOS software. There are no new or modified Cisco IOS commands associated with this feature.

For complete details on the IGMP MIB, see the IGMP-STD-MIB.my file available from the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

IKE—Initiate Aggressive Mode

The IKE—Initiate Aggressive Mode feature allows you to specify RADIUS Tunnel attributes (Tunnel-Client-Endpoint [66] and Tunnel-Password [69]) for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes. This feature is best implemented in a crypto hub-and-spoke scenario, in which the spokes initiate IKE aggressive mode negotiation with the hub by using the preshared keys that are specified as tunnel attributes and stored on the AAA server. This scenario is scalable because the preshared keys are kept at a central repository (the AAA server) and more than one hub router and one application can use the information.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ikeag.htm.

Implementing OSPF for IPv6

The Open Shortest Path First (OSPF) Version 3 for IPv6 (RFC 2740) feature expands on OSPF to provide support for IPv6 routing prefixes. In OSPF for IPv6, the commands used to customize OSPF are in interface configuration mode rather than router configuration mode. When using a nonbroadcast multiaccess (NBMA) interface in OSPF for IPv6, users must manually configure the router in order to detect neighbors.

Integrated IS-IS Multi-Topology Support for IPv6

The Integrated IS-IS Multi-Topology Support for IPv6 feature provides support for routing IPv6 prefixes in Intermediate System-to-Intermediate System (IS-IS) using a multi-topology solution.

Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media

When a network consists of only two networking devices that are connected to broadcast media and using the integrated IS-IS protocol, it is better for the system not to have to handle the link as a broadcast link but rather as a point-to-point link. The Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftissp2p.htm

ROS nº 03/2005 - CN
CPMI - CORREIOS
0512
Fls Nº
3690
Doc.

Integrated IS-IS Support for IPv6

IPv6 supports Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). Routing Information Protocol (RIP) and Integrated Intermediate System-to-Intermediate System (IS-IS) protocols are the supported IGPs for IPv6. Multiprotocol Border Gateway Protocol (BGP) is the supported EGP for IPv6.

IS-IS in IPv6 functions the same as and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and Open System Interconnection (OSI) routes. Extensions to the IS-IS CLI allow configuration of IPv6-specific parameters. IS-IS in IPv6 extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6s.htm

Interactive Voice Response Version 2.0 on Cisco VoIP Gateways

IVR Version 2.0 is the fourth release of IVR and TCL scripting on Cisco IOS VoIP gateways. The Cisco IVR feature (first made available in Cisco IOS Release 12.0(3)T and 12.0(7)T) provides IVR capabilities using TCL scripts.

IVR is a term that is used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly dual tone multifrequency (DTMF) signaling. For example, when a user makes a call with a debit card, an IVR application is used to prompt the caller to enter a specific type of information, such as a PIN. After playing the voice prompt, the IVR application collects the predetermined number of touch tones (digit collection), forwards the collected digits to a server for storage and retrieval, and then places the call to the destination phone or system. Call records can be kept and a variety of accounting functions performed.

The IVR application (or script) is a voice application designed to handle calls on a voice gateway, which is a router that is equipped with Voice over IP (VoIP) features and capabilities.

The IVR feature allows an IVR script to be used during call processing. The scripts interact with the IVR software to perform the various functions. Typically, IVR scripts contain both executable files and audio files that interact with the system software.

IVR Version 2.0 is made up of several separate components in the section that follows. These new features include:

- Media Gateway Control Protocol (MGCP) scripting package implementation
- Real Time Streaming Protocol (RTSP) client implementation
- New Tool Command Language (TCL) verbs to utilize RTSP and MGCP scripting features
- IVR prompt playout and digit collection on IP call legs
- Performance improvements and TCL infrastructure changes
- IVR application MIB for network management

These features add scalability and enable the IVR scripting functionality on VoIP call legs. In addition, support for RTSP enables VoIP gateways to play messages from RTSP-compliant announcement servers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/12_2t/pulskynx.htm

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0513
3690
Doc

Interactive Voice Response Version 2.0 on VoIP Gateways

Interactive Voice Response (IVR) consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR applications can be assigned to specific ports or invoked on the basis of dialed number identification service (DNIS). An IP Public Switched Telephone Network (PSTN) gateway can have several IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the various callers.

IVR systems provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly, dual tone multifrequency (DTMF) signaling. IVR uses Tool Command Language (TCL) scripts to gather information and to process accounting and billing.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ivr72.htm

Note This feature was originally introduced in Cisco IOS Release 12.1(3)T. This release is porting the feature into the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

Interface Alias Long Name Support

The Interface Alias (ifAlias) is a user-specified description of an interface used for SNMP network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to "name" an interface. The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode, or by using a Set operation from a Network Management System.

Before Cisco IOS Release 12.2(2)T, ifAlias descriptions for subinterfaces were limited to 64 characters. A new Cisco IOS software command, **snmp ifmib ifalias long**, configures the system to handle ifAlias descriptions of up to 256 characters. IfAlias descriptions appear in the output of the **show interfaces** CLI command. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm

Interface Index Display

The Interface Index (IfIndex) is a user-specified identification number for an interface used in SNMP network management. The IfIndex is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to consistently identify an interface. A new Cisco IOS software command, **show snmp mib ifmib ifindex**, allows the user to display the IfIndex identification numbers assigned to interfaces and subinterfaces using the CLI. The IFIndex provides a way to display these values without the need for a Network Management Station. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm

Interim Local Management Interface (ILMI)

The Interim Local Management Interface (ILMI) is a protocol defined by the ATM Forum for setting and capturing physical layer, ATM layer, virtual path, and virtual circuit parameters on ATM interfaces. ILMI uses simple network management protocol (SNMP) messages without User Datagram Protocol (UDP) and IP, and organizes managed objects into the following four management information bases (MIBs).

Interim Update at Call Connect

With this feature, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and backward-call-indicators) available at the time of call connection are sent through this interim updated accounting record.

ROS nº 03/2005 - CN
Fls. 0514
Doc. 3690

Interim-Interswitch Signaling Protocol (IISP)

The Interim-Interswitch Signalling Protocol (IISP) defines a static routing protocol (using manually configured prefix tables) for communication between ATM switches. IISP provides support for switched virtual circuits (SVCs) on ATM switches that do not support the Private Network-to-Network Interface (PNNI) protocol.

Interworking Signaling Enhancements for H.323 and SIP VoIP

The Interworking Signaling Enhancements for H.323 and SIP VoIP feature enables VoIP networks to properly signal the setup and tear-down of calls when interworking with PSTN networks. These enhancements ensure that in-band tones and announcements are generated when needed so that the voice path is cut-through at the appropriate point of call setup and that early alerting (ringing) does not occur. In addition, support for network-side ISDN and the reducing of speech clipping is addressed.

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

IP Header Compression Enhancement—PPPoATM and PPPoFR Support

In Cisco IOS Release 12.2(2)T, IP header compression (TCP and IP/UDP/RTP) is now supported on PPP-over-ATM interfaces and PPP-over-Frame Relay interfaces. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt6/qcflem.htm

IP Multicast MIB Enhancements

This feature enhances the IP multicast routing protocol in Cisco IOS software by adding MIB variables to query the number of (S, G) and (*, G) entries. It also adds support for high-speed interface counters.

IP-FORWARDING-TABLE-MIB

This release introduces support for the new IP-FORWARD-MIB (IP Forwarding Table MIB). The current version of the IP Forwarding Table MIB is defined in RFC 2096. (RFC 2096 replaces RFC 1354.) The Cisco implementation of this MIB does not support the ipCiderRouteNextHopAS object. Additionally, all entries for the ipCidrRouteTos object (the IP Type-of-Service field) remain set to zero, which indicates a default TOS policy.

For details, refer to the IP-FORWARD-MIB.my file, available through the Cisco MIB FTP site at the following location:

ftp://ftp.cisco.com/pub/mibs/v2/

IPMROUTE-STD-MIB

This feature introduces support for the IPMROUTE-STD-MIB in Cisco IOS software. IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for management of IP multicast routing in a manner independent of the specific multicast routing protocol in use. Support for this MIB replaces the draft form of the IPMROUTE-MIB.

The IPMROUTE-STD-MIB supports all the MIB objects of the IPMROUTE-MIB and in addition supports the following four new MIB objects:

1. ipMRouteEntryCount
2. ipMRouteHCOctets
3. ipMRouteInterfaceHCInMcastOctets
4. ipMRouteInterfaceHCOutMcastOctets

The ipMRouteScopeNameTable MIB object is not supported because it is not relevant to multicast routers.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0515
3690
Doc.

IPSec and 3DES Feature Set for Cisco 820 Series Routers

The Internet Protocol Security (IPSec) feature is available on the Cisco 820 series routers. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

- IPSec
- Internet Key Exchange (IKE)
- Data Encryption Standard (DES)
- Message Digest 5 (MD5)
- Secure Hash Algorithm (SHA)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

IPSec services are similar to those provided by Cisco Encryption Technology (CET), a proprietary security solution introduced in Cisco IOS Release 11.2. (The IPSec standard was not yet available at Release 11.2.) It provides network data encryption at the IP packet level and implements the following standards:

- Digital Signature Standard (DSS)
- Diffie-Hellman (DH) public key algorithm
- Data Encryption Standard (DES)

IPSec provides a more robust security solution and is standards-based. IPSec also provides data authentication and antireplay services in addition to data confidentiality services, and CET provides only data-confidentiality services.

The following component technologies are implemented for IPSec:

- DES is used to encrypt packet data.
- Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
- MD5 and SHA are hash algorithms.

Triple Data Encryption Standard Feature Set for Cisco 820 Series Routers

The Triple Data Encryption Standard (3DES) Cisco IOS feature is available on Cisco 820 series routers. This feature encrypts packet data. Cisco IOS software implements the mandatory 56-bit DES-Cipher Block Chaining (CBC) with an Explicit initialization vector (IV).

IRR Triggers for GKTMP

The IRR Triggers for GKTMP feature allows a Cisco Gateway to send an information request response (IRR) to the Gatekeeper (GK) containing the details of a particular call after a successful connect. The feature also allows a back end application to set triggers for this message and the GK to deliver the IRR information to the application.

ISDN and V.120 Support for NextPort DSPs

The ISDN and V.120 Support For NextPort DSPs feature provides full coverage for digital calls and performance enhancement for V.120 calls. The feature permits terminating synchronous ISDN and V.120 sessions without customer intervention. This feature allows the Cisco AS5350 and Cisco AS5400 to terminate more than 256 ISDN sessions per channelized T3 (CT3) controller by adding ISDN capacity. This feature is mandatory for wholesale dial installations in which ISDN is being used. This feature permits V.120 calls to operate on the NextPort digital signal processor (DSP) instead of on the CT3 controller to reduce activity on the CPU and to increase the V.120 call capability. Support for these enhancements is automatic, and no configuration steps are required.

0516
3690

ISDN Progress Indicator Support for SIP Using 183 Session Progress

The ISDN Progress Indicator Support for SIP Using 183 Session Progress feature adds the SIP 183 Session Progress and Ringing messages to better map to the ISDN/CAS messages.

ISIS: Allows BGP to Control the Configuration of the Overload Bit

The Intermediate-System to Intermediate-System (IS-IS) protocol defines a special bit in each link-state packet (LSP) called the overload-bit. IS-IS uses the overload bit to "tell" other routers to ignore this router in their shortest path first (SPF) calculations. This function prevents transit traffic from passing through the router before the routing table has converged, and transit traffic is not lost.

IVR: Enhanced Multilanguage Support

This feature releases the infrastructure to support Tool Command Language (TCL)-based script interpreters, which allow you to easily add new languages to your router or access server. You can add a new language by creating a TCL script that interprets prompts into a sequence of audio files or silences. The underlying Cisco IOS dynamic prompting code interfaces with the TCL script to translate the message into a sequence of URLs that point to audio files. Then, the Cisco IOS software plays the sequence of audio files as a dynamic prompt. New TCL-script language interpreters operate simultaneously with the current built-in languages: Spanish, Chinese/Mandarin, and English. Adversely, new TCL-script language interpreters can replace one or more of the built-in languages by overwriting the built-in language functionality.

Note This feature does not release any specific TCL scripts.

Note Although the language intelligence comes from a TCL-based language script, once you configure a language any system (TCL IVR 1.0, 2.0, VxML, MGCP, and so on) on your router can use the configured language with little to no change to Cisco IOS software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmultil.htm

Low Latency Queueing

Low Latency Queueing is now supported on Cisco 820 routers. The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic. Information about LLQ is provided in the *Quality of Service Solutions Configuration Guide*. For overview information, refer to the following chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfconmg.htm#xtocid1239530

For configuration instructions, refer to the following chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfwfq.htm#xtocid2836441

Low Latency Queueing with Priority Percentage Support

This feature allows you to configure bandwidth as a percentage within low latency queueing (LLQ). Specifically, you can designate a percentage of the bandwidth to be allocated to an entity (such as a physical interface, a shaped ATM permanent virtual circuit (PVC), or a shaped Frame Relay PVC) to which a policy map is attached. Traffic associated with the policy map will then be given priority treatment. This feature also allows you to specify the percentage of bandwidth to be allocated to nonpriority traffic classes.

0517
3690

This feature modifies two existing commands—**bandwidth** and **priority**. This feature adds a new keyword to the **bandwidth** command—**remaining percent**. The feature also changes the functionality of the existing **percent** keyword. These changes result in the following commands for bandwidth: **bandwidth percent** and **bandwidth remaining percent**. The **bandwidth percent** command configures bandwidth as an absolute percentage of the total bandwidth on the interface. The **bandwidth remaining percent** command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface. This command allows you to specify the relative percentage of the bandwidth to be allocated to the classes of traffic.

This feature also adds the **percent** keyword to the **priority** command. The **priority percent** command indicates that the bandwidth will be allocated as a percentage of the total bandwidth of the interface. You can then specify the percentage (that is, a number from 1 to 100) to be allocated by using the *percentage* argument with the **priority percent** command.

Unlike the **bandwidth** command, the **priority** command provides a strict priority to the traffic class, which ensures low latency to high priority traffic classes. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftllqpct.htm.

Note This feature was originally introduced in Cisco IOS Release 12.0(5)T. This release is porting the feature into the Cisco AS5300 platform.

LZ Software with Hardware Encryption

Before the LZ Software with Hardware Encryption feature was introduced, compression was not supported with the VPN encryption hardware advanced integration module (AIM) and network module (NM); that is, a user had to remove the VPN module from the router and run software encryption with software compression. This feature enables all VPN modules to support LZ compression in software when the VPN module is in Cisco 2600 and Cisco 3600 series routers, thereby, allowing users to configure and compress 2 128Kb/sec streams.

MD5 File Validation

The MD5 File Validation feature allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, execute the verify command using the new "/md5" keyword. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /MD5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch.

A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Media Forking

Media Forking allows the gateway to create multiple streams (or forks) of media associated with a single call and send those streams to multiple destinations, which may include voice portals with speech recognition. Only the original media stream is bidirectional. Additional branches are unidirectional (transmit only), so additional participants are able to hear only the originating caller and not each other.

Fls Nº 3690

14.270 CA.

Each media stream is independently configured and can be a variation of voice only, named telephone event (NTE) only, or voice plus NTE media stream.The content of the media stream is specified in the signaling when the media stream is established.

Although there can be more than one media destination, there is only one signaling destination, which might be the voice portal. The call leg that was originally signaled (for instance, from the originating gateway to the voice portal) is maintained for the life of the session. The media destinations are independent of the signaling destination, so media forks can be added and removed dynamically. The local telephony call leg must be maintained, and up to four media forks, including the destination of the original call, are supported. Fax calls are not supported on any media streams (including the original) when multiple forks are requested. No media forks can be created for a fax call session.

Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay

The MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature adds support for fax relay and DTMF relay with MGCP. This feature provides two modes of implementation for each component: gateway (GW)-controlled mode and call agent (CA)-controlled mode. In GW-controlled mode, GWs negotiate DTMF and fax relay transmission by exchanging capability information in Session Description Protocol (SDP) messages. That transmission is transparent to the CA. GW-controlled mode allows use of the MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature without upgrading the CA software to support the feature. In CA-controlled mode, CAs use MGCP messaging to instruct GWs to process fax and DTMF traffic. For MGCP T.38 Fax Relay, the CAs can also instruct GWs to revert to GW-controlled mode if the CA is unable to handle the fax control messaging traffic; for example, in overloaded or congested networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmgcpfx.htm

Note Fax CODEC up-speeding is not supported.

Note **debug voip rtp** [**all** | *named-event*] — Enables the new debug flag and displays reception.or transmission of RTP named events is not supported on the Cisco AS5850, since the voice packets are CEF and would not be visible on the RSC card.

MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

The MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature implements the following Media Gateway Control Protocol (MGCP) protocols on the supported Cisco media gateways:

- MGCP 1.0 (RFC 2705)
- Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the PacketCable profile of MGCP 1.0 for trunking gateways (TGWs)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mg1.htm

MGCP Basic CLASS and Operator Services

The MGCP BCOS are a set of calling features, sometimes called "custom calling" features, that use MGCP to transmit voice, video, and data over the IP network. These features are usually found in circuit-based networks. MGCP BCOS brings them to the Cisco IOS gateways on packet-based networks.

CPMI – CORREIOS
0519
3690
Doc.

14.269
A.

The MGCP BCOS software is built on the MGCP CAS PBX and AAL2 software package, and supports MGCP 0.1 and the earlier protocol versions Simple Gateway Control Protocol (SGCP) 1.1 and 1.5.

The following MGCP BCOS features are available on Residential Gateways (RGWs) and Business Gateways (BGWs):

- Distinctive power ring
- Visual Message Waiting Indicator
- Caller ID
- Caller ID with Call Waiting
- Call Forwarding
- Ring Splash
- Distinctive Call Waiting Tone
- Message Waiting Tone
- Stutter Dial Tone
- Off-Hook Warning Tone

The following two features can be run as RGW or trunking gateway (TGW) features:

- 911 calls

  This feature is supported in SGCP mode on Cisco 3660 and Cisco AS5300 platforms and in MGCP mode on all five supported platforms.

- Three-Way Calling

  This feature is supported on the Cisco 3660 and Cisco AS5300 TGW platforms and on the Cisco MC3810 series, and Cisco 2600 RGW platforms. This feature cannot be supported on the G.728 and G.723 codecs.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm

MGCP CAS PBX and AAL2 PVC with Basic CLASS and Operator Services

The MGCP CAS PBX and AAL2 PVC software package is a solutions-oriented program that focuses on several customer gateway scenarios. These scenarios require features that address residential, business, and trunking gateway needs on a variety of hardware platforms:

- Residential cable connectivity
- CAS and analog PBX connectivity
- Incoming CAS support for trunking gateways that support operator services such as busy-line verify and barge-in xGCP support of Voice over ATM Adaption Layer type 2 (VoAAL2)

To answer these needs, the MGCP CAS PBX and AAL2 PVC feature combines and expands existing feature sets on the merged Simple Gateway Control Protocol (SGCP)/MGCP software platform as follows:

- Voice over IP (VoIP) support of selected channel-associated signaling (CAS) features
- SGCP AAL2 features

Refer to the following documents for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcptk.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm

ROS nº 03/2005 - CN
CPMI - CORREIOS
0520
Fls/Nº
Doc 3690

14.268
A.

MGCP Generic Configuration Support for Call Manager (IP-PBX)

The MGCP Generic Configuration Support for Call Manager (IP-PBX) feature provides generic configuration support for Cisco IOS Media Gateway Control Protocol (MGCP) gateways with Call Manager. The gateways receive voice configuration from Call Manager by way of an eXtensible Markup Language (XML) file that is downloaded from a TFTP server.

MGCP Line Package Enhancements for Loop Current Feed Open (LCFO)

The MGCP Line Package Enhancements for Loop Current Feed Open (LFCO) feature enhances Media Gateway Control Protocol (MGCP) residential gateway capabilities to support the generation of the LFCO signal at the request of the call agent. LFCO is a new signal in the line package. This enhancement supports call flows that involve answering machines or other automated devices that act as the terminating party and will facilitate the notification of the originating party's on-hook to such devices. There is no explicit configuration required to enable this feature.

MGCP PRI Backhaul and T1-CAS Support for Call Manager (IP-PBX)

ISDN PRI backhaul provides a method for transporting complete IP telephony signaling information from an ISDN PRI interface of an MGCP voice gateway to Cisco CallManager through a highly reliable TCP connection.

This feature works by terminating all the ISDN PRI Layer 2 (Q.921) signaling functions in the Cisco IOS software on the MGCP voice gateway while, at the same time, packaging all the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to the Cisco CallManager through an IP tunnel over a highly reliable TCP connection. This methodology ensures the integrity of the Q.931 signaling information being passed through the network for managing IP telephony devices.

A rich set of user-side and network-side ISDN PRI calling functions is supported by the ISDN PRI backhaul feature. A single TCP connection is used by the gateway to backhaul all the ISDN D channels to Cisco CallManager. The "SAP/Channel ID" parameter in the header of each message identifies individual D channels. In addition to carrying the backhaul traffic, the inherent TCP keepalive mechanism is also used to determine MGCP voice gateway connectivity to an available call agent.

The MGCP voice gateway also establishes a TCP link to the backup (secondary) Cisco CallManager server. In the event of Cisco CallManager switchover, the ISDN PRI backhaul functions are assumed by the secondary Cisco CallManager server. During this switchover, all active ISDN PRI calls are preserved, and the affected MGCP gateway is registered with the new Cisco CallManager server through a Restart-in-Progress (RSIP) message to ensure continued gateway operation.

T1 CAS is supported in non-backhaul fashion and supported CAS signaling types on the Cisco CallManager are E&M, wink-start, and E&M delay-dial. E1 CAS is not supported.

MGCP Voice on Cisco AS5850 Universal Gateway

Although the documents listed below were not written specifically for the Cisco AS5850, they still apply to the Cisco AS5850. MGCP Voice on Cisco AS5850 Universal Gateway include the following features:

FGD-OS 911 Calls

The 911 feature can be run as residential gateway (RGW) or trunking gateway (TGW) feature.

Interactive Voice Response Version 2.0 on Cisco VoIP Gateway

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_skyn.htm

RQS nº 03/2005 - CN
CPMI - CORREIOS
0521
Fls. Nº
3690
Doc.

14.267
A.

Note The Configuring IVR on the Inbound VoIP Dial Peer feature and the IVR Prompts Played on IP Call Legs feature is not supported.

Media Gateway Control Protocol Residential Gateway Support

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/mgcp1213.htm

MGCP VoIP Call Admission Control

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_04mac.htm

Network Access Server Package for Media Gateway Control Protocol

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_mgnas.htm

PRI/Q.931 Signaling Backhaul for Call Agent Applications

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/ios_121/0144cors.htm

MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mg1.htm

Further Documentation

Refer to the following document for further information about the MGCP Voice on Cisco AS5850 Universal Gateway feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/pull_daz.htm

MGCP VoIP Call Admission Control

The MGCP VoIP Call Admission Control (CAC) feature determines if calls can be accepted on the IP network on the basis of available network resources. Before this release, Media Gateway Control Protocol (MGCP) Voice over IP (VoIP) calls were established regardless of the available resources on the gateway or network. The gateway had no mechanism for gracefully refusing calls if resources were not available to process the call. New calls would fail with unexpected behavior and in-progress calls would experience quality-related problems.

The MGCP VoIP Call Admission Control feature provides three CAC mechanisms to address the need for improved quality and predictable gateway behavior. The first mechanism is local/system CAC, which provides the ability to gracefully refuse calls on the basis of the availability of local gateway call processing resources such as CPU utilization and memory. The second CAC mechanism provides synchronization with Resource Reservation Protocol (RSVP) and reports the reservation request to the call agent. The third mechanism provides network congestion detection to gracefully refuse calls on the basis of a measured level of congestion.

The MGCP VoIP Call Admission Control feature was previously released in Cisco IOS Release 12.2(8)T and is now supported on the Cisco 1751 and Cisco 1760 platforms.

CPMI - CORREIOS
0522
Fls Nº
3690
Doc.

14266
A.

MGCP VoIP Signaling for 1750 Series

The MGCP CAS PBX and AAL2 PVC features extend the earlier Simple Gateway Control Protocol (SGCP) Channel Associated Signaling (CAS) and AAL2 support onto the merged SGCP/MGCP software base to enable various service provider solutions. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftmgcpba.htm

Mobile IP —IPSec for Home Agent to Foreign Agent Tunnel

The Mobile IP—IPSec for Home Agent to Foreign Agent Tunnel enables the use of IPSec on the home agent to foreign agent tunnel.

Crypto map configuration must be applied to both the tunnel and physical interfaces. For details refer to the "Configuring Cisco Encryption Technology" chapter in the Release 12.2 *Cisco IOS Security Configuration Guide*.

Mobile IP MIB Support for SNMP

The Mobile IP MIB Support for SNMP feature adds a MIB module which expands network monitoring capabilities of Foreign Agent (FA) and Home Agent (HA) Mobile IP Entities. Mobile IP management using SNMP is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB. The Cisco Mobile IP MIB is a Cisco enterprise-specific extension to IETF RFC 2006 MIB module which allows you to monitor the total number of HA Mobile bindings and the total number of FA visitor bindings. This release also adds support for RFC 2006 Set operations and a SNMP notification. Set operations (performed from a Network Management System) are supported for starting and stopping the mobile IP service, configuring security associations, modifying advertisement parameters, and configuring "care-of addresses" for foreign agents. An SNMP notification (trap or inform) for security violations can be enabled on supported routing devices using the **snmp-server enable traps ipmobile** and **snmp-server host** global configuration CLI commands. As this feature affects security, use of SNMPv3 is strongly recommended.

For further details, refer to the *Mobile IP MIB Support for SNMP* Feature Guide at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft1mip.htm

Mobile IP—Fastswitching Support on Foreign Agent

The Mobile IP—Fastswitching Support on Foreign Agent feature enables packets to be fast switched from the foreign agent both in the direction of the mobile node and through the reverse tunnel. In the direction of the mobile node, packets will be properly fast-switched for global IP addresses. However, this feature does not support fast-switching to mobile nodes using private home addresses.

Fast-switching packets through the reverse tunnel is achieved by intercepting packets before cache lookup and dynamically switching them through the correct tunnel interface.

Mobile IP—Generic NAI Support and Home Address Allocation

The Mobile IP—Generic NAI Support and Home Address Allocation feature allows a mobile node to be identified by using a network access identifier (NAI) instead of an IP address (home address). The NAI is a character string similar to an email address in that it is formatted as either *user* or *user@realm* but it need not be a valid e-mail address.

The original purpose of the NAI was to support roaming between dialup ISPs. With the NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each realm.

These services are also valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. The mobile node can identify itself by including the NAI along with the Mobile IP registration request.

CPMI - CORREIOS
0523
3690

Additionally, this feature allows you to configure the home agent to allocate addresses to mobile nodes either statically (including multiple static addresses per NAI flow) or dynamically. Home address allocation can be from address pools configured locally, through either DHCP server access, or from the AAA server.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnaiadd.htm

Mobile IP—MIB Support for NAI and HA Redundancy

The CISCO-MOBILE-IP-MIB is enhanced to add support for following features:

1. Compliance with RFC 2794 for mobile nodes identified by Network Access Identifiers (NAI).

The following tables are defined in the MIB to support NAI based mobile nodes (MN):

- cmiFaRegVisitorTable
- cmiHaRegCounterTable
- cmiSecAssocTable
- cmiSecViolationTable

These tables are the same as the corresponding tables in the RFC2006-MIB (MIP MIB) in terms of the information they provide, but indices are changed so that entries for mobile nodes which are not identified by the IP address will also be included in the table.

The 'cmiHaRegMobilityBindingTable' is augmented from 'haMobilityBindingTable' of the RFC2006-MIB (MIP MIB) to provide the NAI information.

2. HA redundancy feature.

Scalar objects have been added to MIB to monitor the message exchanges between peer home agents. These objects are under the 'cmiHaRedun' subtree of the MIB.

3. Performance monitoring.

There are scalar objects under 'cmiHaReg' subtree which gives statistics about the registration processing rate at home agent. Distinction is made between registration requests authenticated locally and those authenticated at the AAA server. There are scalar objects under the 'cmiMaReg' subtree which give statistics about the rate at which registration requests are received at the mobility agent (HA or FA).

Mobile IP—Private Addressing Support

The Mobile IP—Private Addressing Support feature allows the use of private IP addresses for mobile nodes. Enhancements have been made to the foreign agent to allow it to distinguish between mobile nodes using the same private home address, but with different home agents.

When a mobile node successfully registers with a foreign agent, a tunnel is set up between the foreign agent and the home agent. When a packet is received by the foreign agent for the mobile node, the foreign agent will identify which mobile node to route the packet to based on the address of the mobile node, as well as the home agent from which the packet came.

Mobile Networks

The Cisco Mobile Networks feature enables a Mobile Router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this Mobile Router.

Mobile IP, as defined in standard RFC 2002, provides the architecture that enables the Mobile Router to connect back to its home network. Mobile IP allows a device to roam while appearing to be at its home network. Such a device is called a mobile node. A mobile node is a node, for example, a personal digital assistant, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and maintain ongoing communications while using the same IP address.

The Mobile Router functions similarly to the mobile node with one key difference—the Mobile Router allows entire networks to roam. For example, a plane with a Mobile Router can fly around the world while passengers stay connected to the Internet. This communication is accomplished by Mobile IP aware routers tunneling packets, which are destined to hosts on the mobile networks, to the location where the Mobile Router is visiting. The Mobile Router then forwards the packets to the destination device.

These devices can be mobile nodes running Mobile IP client software or nodes without the software. The Mobile Router eliminates the need for a Mobile IP client. In fact, the nodes on the mobile network are not aware of any IP mobility at all. The Mobile Router "hides" the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

The Cisco Mobile Networks feature is a static network implementation that supports stub routers only. The Mobile Router avoids convergence problems by statically defining which networks it can address. The Mobile Router can do the following:

- Perform agent solicitation
- Perform registration and reregistration
- Decapsulate information for its attached devices

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm

Mobile Networks MIB Support

The Cisco Mobile Networks MIB Support feature implements mobile node MIB groups for the monitoring and management of Cisco Mobile Network activity. Data from managed objects is returned through the use of the "show" commands described in the documentation for the "Cisco Mobile Networks" 12.2(4)T feature, or can be retrieved from a Network Management System using SNMP.

The Cisco Mobile Networks MIB Support feature implements the following mobile node (mn) groups in the Mobile IP MIB (RFC2006-MIB): the mnSystem group, the mnDiscovery group, and the mnRegistrationGroup.

For further details, refer to the RFC2006-MIB.my file, available through Cisco.com at ftp://ftp.cisco.com/pub/mibs/v2/, and RFC 2206, "The Definitions of Managed Objects for IP Mobility Support using SMIv2."

Modem Script and System Script Support in Large-Scale Dial-Out

Modem connection and system login chat scripts are often used when asynchronous dial-on-demand routing (DDR) is configured. Currently, however, the large-scale dial-out network architecture does not allow chat scripts for a particular session to be passed through the network. Cisco IOS Release 12.2(2)T allows modem and system chat scripts to pass through large-scale dial-out networks by allocating two new authentication, authorization, and accounting (AAA) attributes for outbound service.

The AAA attributes define specific AAA elements in a user profile. Large-scale dial-out supports Cisco attribute-value (AV) pairs and TACACS+ attributes. The Modem Script and System Script Support in Large-Scale Dial-Out feature provides two new outbound service attributes for passing chat scripts: modem-script and system-script. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftlschat.htm

MPLS Over ATM: Virtual Circuit (VC) Merge

VC merge maps several incoming labels to one single outgoing label. Cells from different virtual channel identifiers (VCIs) that travel to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections.

VC merge allows the switch to transmit cells that come from different VCIs over the same outgoing VCI to the same destination. In other words, VC merge queues ATM Adaptation Layer 5 (AAL5) frames in input buffers until the switch receives the last frame. Then the switch transmits the cells from that AAL5

CPMI - CORREIOS
3690

14-263
VA

frame before it sends any cells from other frames. VC merge requires the switch to provide buffering, but no more buffering than is required in IP networks. VC merge slightly delays the transfer of frames; however, VC merge is for IP traffic and not for traffic that requires speed. IP traffic tolerates delays better than other traffic on the ATM network.

MPLS VPN ID

Using Multiprotocol Label Switching (MPLS) VPN ID you can identify virtual private networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the MPLS VPN ID feature is used for identifying a VPN. The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in routing updates.

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftvpnid.htm

Multicast Music on Hold Support for Call Manager (IP-PBX)

The Multicast Music on Hold Support for Call Manager (IP-PBX) feature provides the functionality to stream music from a Multicast Music on Hold (MOH) server to the voice interfaces of on-net and off-net callers that have been placed on hold.

This integrated multicast capability of Cisco CallManager 3.1 is implemented through the H.323 signaling plane in Cisco CallManager.

In an MOH environment, whenever caller A places caller B on hold, Cisco CallManager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets can be relayed to appropriately configured voice interfaces in a VoIP network that have been placed on hold.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be preconfigured in Cisco CallManager and the Cisco IOS MGCP voice gateways.

The MOH feature enables you to subscribe to a music streaming service when using a Cisco IOS MGCP voice gateway. By means of a preconfigured multicast address on a gateway, the gateway can "listen for" Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network.

RTP is the Internet-standard protocol for transporting real-time data across a network, including audio and video information. Thus, RTP is well suited for media on demand and interactive services, such as IP telephony.

The default router in the network for handling multicast traffic must have the following enabled:

- Multicast routing
- A multicast routing protocol, for example Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP)
- An IP routing protocol, for example Routing Information Protocol (RIP) or Open Shortest Path First (OSPF)

When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP) "join" message to the default router, indicating to the default router that the gateway is to receive RTP multicast packets.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0526
3690
Doc

14.262
A-

Multiple RSA Keypair Support

The Multiple RSA Keypair Support feature allows the Cisco IOS software to maintain a distinct key pair for each certification authority (CA) with which it is dealing. Thus, the Cisco IOS software can match policy requirements for each CA without compromising the requirements specified by the other CAs, such as key length, key lifetime, and general-purpose versus special-usage keys.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm

NAT MIB (Read-Only)

This feature introduces support for the Network Address Translation (NAT) MIB. NAT provides tables for translating internal network addresses external network addresses. The NAT MIB provides objects for the monitoring and management of NAT bindings and session using SNMP. In this release, access to the MIB is limited to the read-only level. No new or modified Cisco IOS commands are associated with this MIB.

For details on the management options provided by the MIB, see the CISCO-IETF-NAT-MIB.my file available in the "SNMP v2 MIBs" section of the Cisco.com MIB page at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. Additional information on the MIB is available in the form of an internet draft (draft-ietf-nat-natmib), available through www.ietf.org.

NAT Protocol Translation

Network Address Translation - Protocol Translation (NAT PT) is an IPv6 translation mechanism allowing IPv6-only devices to communicate with IPv4-only devices, and vice versa. NAT PT was designed using RFC 2766 as a migration tool to help customers transition their IPv4 networks to IPv6 networks. Using existing IPv4 NAT capability and adding a protocol translator allows NAT PT to provide direct communication between hosts speaking a different network protocol.

NAT Support of H.323 RAS

Cisco IOS NAT supports all H.225 and H.245 message types, including those sent in the RAS protocol. RAS provides a number of messages that are used by software clients and Voice over IP (VoIP) devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Some RAS messages include IP addressing information in the payload, typically meant to register a user with the gatekeeper or learn about another user already registered. If these messages are not known to NAT, they cannot be translated to an IP address that will be visible to the public.

Previously, NAT did not support H.323 v2 RAS messages. With this enhancement, embedded IP addresses can be inspected for potential address translation.

AT-Support of H.323 v2 Call Signaling

Cisco IOS NAT supports all H.225 and H.245 message types, including FastConnect and Alerting, as part of the H.323 v2 specification.

Previously, NAT only supported H.323 version 1 and that was specific only to the Microsoft NetMeeting application. With this enhancement, any product that makes use of these message types will be able to pass through a Cisco IOS NAT configuration without any static configuration.

This feature was previously released in Cisco IOS Release 12.1(5)T on the Cisco Catalyst 2900, Cisco Catalyst 2900XL, Cisco Catalyst 4000 series, Cisco Catalyst 5000 family switches with an installed Route Switch Module, Cisco Catalyst 6000 series, Cisco Catalyst 8500 series, Cisco LightStream 1010 series, Cisco 800 series, Cisco 1000 series, Cisco 1400 series, Cisco 1600 series, Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 4000 series, Cisco AS5300, Cisco AS5400, Cisco AS5800, Cisco 6400 series, Cisco 7000 series, Cisco 8500 series, Cisco 12000 series, Cisco MC3810, Cisco uBR900, and Cisco uBR7200 platforms. This release is porting the feature into the Cisco IAD2420 platform.

CPMI - CORREIOS
0527
Fls. Nº
3690

14.261
A.

NetFlow Multiple Export Destinations

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data by providing redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets will be lost. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dtnfdest.htm

NetFlow ToS-Based Router Aggregation

The NetFlow ToS-Based Router Aggregation feature provides the ability to enable limited router-based type of service (ToS) aggregation of NetFlow Export data, which results in summarized NetFlow Export data to be exported to a collection device. The result is lower bandwidth requirements for NetFlow Export data and reduced platform requirements for NetFlow data collection devices. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm

NetWare Link Services Protocol (NLSP)

The NetWare Link Services Protocol (NLSP) will no longer be offered after Cisco IOS Release 12.2(13)T. NLSP commands will not appear in future releases of the Cisco IOS software documentation set.

Network Access Server (NAS) Package for MGCP

The Network Access Server (NAS) Package for MGCP feature adds support for the Media Gateway Control Protocol (MGCP) NAS package on the Cisco AS5350, Cisco AS5400, and Cisco AS5850. With this implementation, data calls can be terminated on a trunking media gateway that is serving as a NAS. Trunks on the NAS are controlled and managed by a call agent that supports MGCP for both voice and data calls. The call agent must support the MGCP NAS package.

These capabilities are enabled by the universal port functionality of the Cisco AS5350, Cisco AS5400, and Cisco AS5850, which allows these platforms to operate simultaneously as network access servers and voice gateways to deliver universal services on any port at any time. These universal services include dial access, real-time voice and fax, wireless data access, and unified communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_mgnas.htm

No Service Password-Recovery

The No Service Password-Recovery feature disables password-recovery capability for better console security.

Nonblocking Gatekeeper AAA Interface

The Nonblocking Gatekeeper AAA Interface feature enables Cisco gatekeepers to perform authentication, authorization, and accounting (AAA) through the gatekeeper interface at much higher call rates.

There are no new or modified commands.

OSPF Sham-Link Support for MPLS VPN

A sham link is a logical path within an Open Shortest Path First (OSPF) area; it represents an unnumbered point-to-point connection between two provider edge (PE) devices. All routers within the area see the link and use it during the shortest path first (SPF) computation.

ECT nº 03/2006 - CN
CPMI - CORREIOS
Fls. 0328
3690
Doc.

On PE routers the VPN Route Forwarding (VRF) routing table is populated by OSPF routes over the sham link. The sham link gives users the capability of specifying which path will be used for traffic.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ospfshmk.htm

Particle Drivers

The Particle Drivers feature is a collection of performance and reliability improvements for the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways. It includes particles-based packet drivers for improved performance. These particle drivers optimize Cisco IOS fast switching code and significantly improve the way Cisco IOS uses processor cache memory. Data packets for some protocols, such as MLPPP, IP Multicast, and cRTP, are fast switched with particle drivers. Cisco IOS CEF switching paths are highly optimized with particle drivers.

PIM MIB Extension for IP Multicast

Protocol Independent Multicast (PIM) is an IP Multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the *Protocol Independent Multicast for IPv4* MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

The PIM MIB Extension for IP Multicast feature introduces support in Cisco IOS software for the CISCO-PIM-MIB, which is an extension of RFC 2934 and an enhancement to the existing Cisco implementation of the PIM MIB. This feature introduces the following new classes of PIM notifications:

- neighbor-change—This notification results from the following conditions:
  - When the PIM interface of a router is disabled or enabled (using the **ip pim** command in interface configuration mode).
  - When the PIM neighbor adjacency of a router expires or is established (defined in RFC 2934).
- rp-mapping-change—This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
- invalid-pim-message—This notification results from the following conditions:
  - When an invalid (*, G) join or prune message is received by the device (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group).
  - When an invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftpimmib.htm

PIM Multicast Scalability

The PIM Multicast Scalability feature enhances the Protocol Independent Multicast (PIM) protocol in Cisco IOS software by adding a new level of scalability. With this feature, edge devices can have a large number of multicast groups and users without increasing the CPU utilization of the router.

Plain NFAS Support on NM-HDV

The current Non-Facility Associated Signaling (NFAS) support on the High-Density Voice network modules (NM-HDV) is joined with the Redundant Link Manager/Signaling System 7 (RLM/SS7). When a user configures an ISDN PRI NFAS group via the Cisco command line interface (CLI), all channels within the PRI are treated as B channels. A D channel is not created and, thus no signaling will be passed to the ISDN stack.

This feature modifies the existing implementation of NFAS/RLM on NM-HDV to activate the generic NFAS feature on Cisco 2600 and 3600 routers and to allow the coexistence of plain NFAS and NFAS/RLM/SS7 on the Cisco 3660 router.

14259 A.

PPPoE Connection Throttling

This feature will throttle the PPP over Ethernet (PPPoE) connection requests to prevent any denial of service attacks. It will implement per-mac/per-vc initiated session rate throttling in the PPPoE server to limit the session initiate count during a specific period of time.

PPPoE MTU Adjustment

The syntax of the **ip adjust-mss** command has changed to the following:

ip tcp adjust-mss *mss*

where the value of the *mss* argument must be 1452 or less to fix the Point-to-Point Protocol over Ethernet (PPPoE) maximum transmission unit (MTU) problem.

PPPoE over Gigabit Ethernet

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces. The PPPoE over Gigabit Ethernet feature is supported on Cisco 7200 series routers with Gigabit Ethernet line cards.

Preauthentication with ISDN PRI and Channel-Associated Signaling Enhancements

Preauthentication allows a Cisco network access server (NAS) to decide—on the basis of the Dialed Number Identification Service (DNIS) number—whether to answer an incoming call. When an incoming call arrives from the public network switch but before it is answered, the NAS sends the DNIS number to a RADIUS server for authorization.

The Preauthentication with ISDN PRI and Channel-Associated Signaling Enhancements feature provides additional support for preauthentication, which was introduced in a previous Cisco IOS release. For more information about preauthentication, refer to the Cisco IOS Release 12.1(3)T feature module titled *Preauthentication with ISDN PRI and Channel-Associated Signaling*.

This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication on the basis of the Calling Line Identification (CLID) number in the same transaction. For more information about attribute 44 and how it works with preauthentication, refer to the Cisco IOS Release 12.0(7)T feature module titled *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt1.htm

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release is porting the feature into the Cisco AS5350 and Cisco AS5850 platforms.

PRI QSIG Protocol

QSIG is a standardized PBX signaling protocol used primarily in Europe over E1 and BRI trunks and occasionally in North America over T1 trunks. The PRI QSIG Protocol feature provides QSIG signalling over PRI trunks.

PSTN Fallback

The goal of PSTN fallback is to monitor congestion in the IP network and either redirect calls to the PSTN or reject calls based on the network congestion. Calls can be rerouted to an alternate IP destination or to the PSTN if the IP network is found unsuitable for voice traffic at that time. The user defines the congestion thresholds based on the configured network. This functionality enables the service provider to give a reasonable guarantee about the quality of the conversation to their VoIP users at the time of call admission.

RRS nº 03/2005 - CN
FLS Nº 0538
Doc 3690

14258
A

Note PSTN fallback does not provide assurances that a VoIP call that proceeds over the IP network is protected from the effects of congestion. This is the function of the other Quality of Service (QoS) mechanisms such as IP Real-Time Transport Protocol (RTP) priority or low latency queuing (LLQ).

PSTN fallback includes the following features:

- Offers flexibility to define the congestion thresholds based on the network.
  - Defines a threshold based on Calculated Planning Impairment Factor (ICPIF), which is derived as part of International Telecommunication Union (ITU) G.113.
  - Defines a threshold based solely on packet delay and loss measurements.
- Uses Service Assurance Agent (SAA) probes to provide packet delay, jitter, and loss information for the relevant IP addresses. Based on the packet loss, delay, and jitter encountered by these probes, an ICPIF or delay and loss values are calculated.
- Is supported by calls of any codec. Only G.729 and G.711 have accurately simulated probes. Calls of all other codecs are emulated by a G.711 probe.

For more information, including configuration tasks and examples, and command references for PSTN fallback, please refer to PSTN Fallback. Refer to the following document for additional information about the Call Admission Control for H.323 VoIP Gateways feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm

RADIUS Attribute 52 and Attribute 53 Gigaword Support

The RADIUS Attribute 52 and Attribute 53 Gigaword Support feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords) in accordance with RFC 2869. Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to "Stop" or "Interim-Update." These attributes can be used to keep accurate track of and bill for usage.

RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

Virtual private networks (VPNs) use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP) or asynchronous High-Level Data Link Control (HDLC)). Internet service providers (ISPs) configure their network access servers (NASs) to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel server—the tunnel endpoint. The customer maintains the IP addresses, routing, and other user database functions of the tunnel server users.

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature adds the ability to specify the host name of the NAS—rather than the IP address of the NAS—in RADIUS attribute 66 (Tunnel-Client-Endpoint). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt4.htm

RADIUS Attribute 77 for DSL

The RADIUS Attribute 77 for DSL feature introduces support for Attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the classname used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.

0531
Fls Nº
3690
Doc

14257
A.

RADIUS Number Translation VSAs for VoIP

The RADIUS Number Translation VSAs for VoIP feature enables a Cisco AS5x00 voice gateway to export pre- and post-translated called and calling numbers to a RADIUS server in the form of generic vendor-specific attributes (VSA). Cisco gateways can be configured to present gateway received, gatekeeper translated, and final translated numbers to the RADIUS server.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm

RADIUS Route Download

The RADIUS Route Download feature allows users to configure their network access server (NAS) to send static route download requests to authentication, authorization, and accounting (AAA) servers specified by a named method list. Before this feature, all RADIUS authorization requests for static route download could be sent only to AAA servers specified by the default method list.

This feature extends the functionality of the **aaa route download** command to allow users to specify the name of the method list that will be used to direct static route download requests to the AAA servers. The **aaa route download** command must be used to add separate method lists; however, users will continue to enable the **aaa authorization configuration default** command to download static route configuration information from the AAA server specified by the default method list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftradrou.htm

Reverse Path Forwarding - Source Exists Only

The Reverse Path Forwarding - Source Exists Only feature allows you to verify if the source IP address is valid in the Forwarding Information Base (FIB) for unicast Reverse Path Forwarding (uRPF) traffic. Packets that have not be allocated on the Internet, being used for spoofed source addresses, will be dropped. Packets with an entry in the FIB will be passed. This uRPF option can be used on internet service provider (ISP) peering routing devices with other ISPs.

Rotating Through Dial Strings

The Rotating Through Dial Strings feature allows you to specify the dialing order when multiple dial strings are configured. Options for dialing order include:

- Sequential—Dial using the first dial string configured in a list of multiple strings.
- Round-robin—Dial using the dial string following the most recently successful dial string.
- Last successful call—Dial using the most recently successful dial string.

This feature takes advantage of information available from a previous call attempt, such as whether the call was unsuccessful or the line was busy, and thereby increases the rate of successful calls.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftrotdls.htm.

RPR+ (Route Processor Redundancy Plus) on Cisco 7500 Series Routers

The RPR+ feature is an enhancement of the RPR feature on Cisco 7500 series routers. RPR+ keeps the Virtual Interface Processors (VIPs) from being reset and reloaded when a switchover occurs between the active and standby Route Switch Processors (RSPs). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/fs22rpr.htm

IRS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0532
Doc 3690

RSVP Support for Low Latency Queueing

Resource Reservation Protocol (RSVP) is a network-control protocol that provides a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across networks achieve the desired quality of service (QoS).

14-253
A.

completion, for SIP status codes or events. The opposite is also true: SIP status codes or events are mapped to PSTN cause codes. Event mapping tables found in this document show the standard or default mappings between SIP and PSTN.

However, you may want to customize the SIP user agent software to override the default mappings between the SIP and PSTN networks. The Configurable PSTN Cause Code to SIP Response Mapping feature allows you to configure specific map settings between the PSTN and SIP networks. Thus, any SIP status code can be mapped to any PSTN cause code, or vice versa. When set, these settings can be stored in the NVRAM and are restored automatically on bootup.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmap.htm

SIP—DNS SRV RFC2782 Compliance

Session Initiation Protocol (SIP) on Cisco Voice over IP (VoIP) gateways uses Domain Name System Server (DNS SRV) query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style, from RFC 2052, has always been available; however, with this release, a second style is also available. The second style complies with RFC 2782 and prepends the protocol label with an underscore "_"; as in "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style. Use the **srv version** command to configure the DNS SRV feature.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/vvfresrv.htm

SIP—Session Initiation Protocol for VoIP

Voice over IP (VoIP) currently implements the ITU H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. Session Initiation Protocol (SIP) is a protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to H.323. The Cisco SIP functionality equips Cisco routers to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within the VoIP internetworking software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sip72.htm

SIP—Session Initiation Protocol for VoIP Enhancements

Voice over IP (VoIP) currently implements the International Telecommunication Union (ITU)'s H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. The Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. SIP features are compliant with IETF RFC 2543, *SIP: Session Initiation Protocol*, published in March 1999.

The Cisco SIP functionality, introduced in Cisco IOS Release 12.1(1)T and enhanced in Cisco IOS Release 12.1(3)T, enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. The SIP feature also provides nonproprietary advantages in the areas of

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

RDS nº 03/2005 - CN
CPMI - CORREIOS
0533
Fls Nº
3690
Doc

14-252
A.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsipgv.htm

SLT Dual Ethernet

The Cisco SLT Dual Ethernet feature adds Cisco SLT dual Ethernet support to the virtual switch controller (VSC). This enhanced Cisco SLT support provides two IP networks and two additional Session Manager sessions (for a total of four Session Manager sessions) for improved backhaul communication. These additions increase the resilience of Cisco SLT/VSC communications by supporting two RUDP sessions from each Ethernet interface to each VSC. These VSC enhancements contribute to determining when to switch Ethernets and when to switch VSC activity.

The Cisco SLT, which is based on the Cisco 2611 Multi-Service Access Router, is shipped with two Ethernet interfaces. Until this feature was released, the Cisco SLT/VSC solution supported only one of the two Ethernet interfaces. Both Session Manager sessions needed to travel over this single Ethernet interface: This Ethernet was a single-point failure. The Cisco SLT Dual Ethernet feature supports the second Ethernet, which improves the resilience of the backhaul IP communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftsltdes.htm

SLT G.732 Support

The Cisco SLT enables service providers to reliably transport Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 SLT feature set, providing reliable interoperability with the Cisco SC2200 or the Cisco VSC3000 device. The Cisco SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using the Cisco Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports, upper-layer SS7 protocols across an IP network to the Cisco SC2200 or VSC3000 device. The Cisco SLT is supported only on the Cisco 2611 router.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_g732.htm

SNMP IF-MIB Support for VLAN (ISL, 802.1Q) Subinterfaces

This feature updates the Cisco implementation of the Interfaces Group MIB (abbreviated "IF-MIB" and defined in RFC 2233) to completely support ifTable and ifXTable entries for Inter-Switch Link (ISL) or 802.1Q encapsulated subinterfaces.

The Interface Table (the ifTable object) contains information on an Simple Network Management Protocol (SNMP) management entity's interfaces. Each sublayer of a network interface is considered to be an interface. An ifTable is a list of interface entries in which each entry contains management information applicable to that interface. The ifXTable is an extension to the ifTable. It contains replacements for objects of the ifTable that were deprecated. The ifXTable also contains 64-bit versions of the counters defined in the ifTable. Cisco IOS software can support both interfaces and subinterfaces in the ifTable.

ISL is a Cisco protocol for interconnecting switches and maintaining VLAN information as traffic is exchanged between switches. It can also be used to configure routing between any number of VLANs in a network by creating subinterfaces for each VLAN.

802.1Q (also referred to as "DOT1Q") is an IEEE standard protocol for interconnecting bridges/switches and maintaining VLAN information as traffic is exchanged between the devices. 802.1Q can also be used to configure routing between any number of VLANs in a network by creating subinterfaces for each VLAN.

The following objects of the ifTable have been updated: ifIndex, ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress, ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts.

ECT/ANO 0534
Doc. 3690

The following objects of the ifXTable have been updated:

- ifName
- ifInMulticastPkts
- ifInBroadcastPkts
- ifOutMulticastPkts
- ifOutBroadcastPkts
- ifHCInOctets
- ifHCInUcastPkts
- ifHCInMulticastPkts
- ifHCInBroadcastPkts
- ifHCOutOctets
- ifHCOutUcastPkts
- ifHCOutMulticastPkts
- ifHCOutBroadcastPkts.

SNMP Support over VPN

The SNMP Support over VPN feature allows the sending and receiving of SNMP notifications using VPN Routing Forwarding table (VRF).

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A VPN is a network that provides high connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet or on the service provider IP, Frame Relay, or ATM system.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, guidelines, and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support over VPN feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftnm_vpn.htm

SNMPv3 Community MIB Support

The SNMPv3 Community MIB Support feature implements support for the SNMP Community MIB (SNMP-COMMUNITY-MIB) module, defined in RFC 2576, in Cisco IOS software.

The SNMPv1/v2c Message Processing Model and Security Model require mappings between parameters used in SNMPv1 and SNMPv2c messages and the version independent parameters used in the Simple Network Management Protocol (SNMP) architecture. The SNMP Community MIB contains objects for mapping between these community strings and version-independent SNMP message parameters.

The mapped parameters consist of the SNMPv1/v2c community name and the SNMP securityName and contextEngineID/contextName pair. This MIB provides mappings in both directions, that is, a community name may be mapped to a securityName, contextEngineID, and contextName, or the combination of securityName, contextEngineID, and contextName may be mapped to a community name. This MIB also augments the snmpTargetAddrTable with a transport address mask value and a maximum message size value.

RCVD IP 03/2003 - CN
Doc. 3690

14.250
A.

For implementation details, refer to the SNMP-COMMUNITY-MIB.my file, available through Cisco.com at ftp://ftp.cisco.com/pub/mibs/v2/

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0536
Doc. 3690

14.249
A.

Speech Recognition and Synthesis for Voice Applications

The Speech Recognition and Synthesis for Voice Applications feature adds support for automatic speech recognition (ASR) and text-to-speech (TTS) capabilities for VoiceXML and TCL applications. This feature provides interfaces to ASR and TTS media servers using Media Resource Control Protocol (MRCP), an application-level protocol developed by Cisco and its ASR and TTS media server partners. Client devices that process audio or video streams use MRCP to control media resources on the external ASR and TTS servers.

Refer to the following documents for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/vxmlprg/index.htm

Static Cache Entry for IPv6 Neighbor Discovery

The Static Cache Entry for IPv6 Neighbor Discovery feature enables the configuring of static entries in the IPv6 neighbor discovery cache, which provides functionality in IPv6 that is equivalent to static Address Resolution Protocol (ARP) entries in IPv4. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process. Cisco IOS software uses static ARP entries in IPv4 to translate 32-bit IP addresses into 48-bit hardware addresses. In IPv6, Cisco IOS software uses static entries in the IPv6 neighbor discovery cache to translate 128-bit IPv6 addresses into 48-bit hardware addresses.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6s.htm

Supplementary Telephone Services for the Euro-ISDN Switch

The Cisco 800 series routers now support the following plain old telephone service (POTS) features for the European Telecommunications Standards Institute (ETSI) Euro-ISDN switch type:

- Caller ID presentation and restriction are available for Denmark, Finland, and Sweden.
- Calling line identification restriction (CLIR) temporarily prevents your calling ID from being presented to the destination number for an outgoing call. You must configure CLIR prior to each call in which you want to restrict the calling party number from being presented at the destination.
- Call forwarding is enabled using Cisco IOS and dual tone multifrequency (DTMF) keypad commands.
- Call transfer enables you to connect two call destinations. The request for this service must originate from an active, outgoing call.

Note The Euro-ISDN switch was previously called the NET3 switch.

- The following types of voice call forwarding services are supported on the Euro-ISDN switch:
  - Call forward unconditional (CFU) redirects your calls without restrictions and takes precedence over other call forwarding types.
  - Call forward busy (CFB) redirects your call to another number if your number is busy.
  - Call forward no reply (CFNR) forwards your call to another number if your number does not answer within a specified period of time.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftv800.htm

ECT nº 03/2006 - CN
CPMI - CORREIOS
Fls Nº 0537
Doc. 36-90

14.248
A.

T.37 for Cisco 7200

This feature adds T.37 standards-based store-and-forward fax protocol support for H.323 gateways and gatekeepers to the Cisco 7200 series. T.37 is an ITU-T recommended standard for store-and-forward fax that enables Cisco gateways and gatekeepers to interwork with other Cisco gateways and third-party H.323 devices that support the T.37 protocol.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm

T.37 store-and-forward fax was originally supported in Cisco IOS Release 12.1(5)T on the Cisco AS5300 platform. In Cisco IOS Release 12.2(8)T, support was added on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745. In Cisco IOS Release 12.2(13)T, support was added on the Cisco AS5350 and the Cisco AS5400. Cisco IOS Release 12.2(15)T adds support on the Cisco 7200 series.

T.38 Fax Relay for VoIP H.323

The T.38 Fax Relay for VoIP H.323 feature provides standards-based Fax Relay protocol support on Cisco 2600 series, Cisco 3600 series, Cisco 7200 series and Cisco MC3810 series multiservice gateways. The Cisco proprietary Fax Relay solution is sometimes not an ideal solution for Enterprise and Service Provider customers who have implemented a mixed vendor network. Because the T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers will now be able to interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed vendor network where real time Fax Relay capabilities are required.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm

Note This feature was originally introduced in Cisco IOS Release 12.1(3)T. This release ports the feature into the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

T1 Channel Associated Signaling (CAS)

Channel Associated Signaling (CAS) is the transmission of signaling information within the voice channel. Support for CAS is now available on T1 interfaces.

TCL IVR 2.0 Call Initiation and Callback

The TCL IVR 2.0 Call Initiation and Callback feature allows Tool Command Language (TCL) Interactive Voice Response (IVR) applications to make outbound calls without specifying an incoming call leg in the setup command.

The TCL IVR 2.0 Call Initiation and Callback feature modifies the following TCL IVR Version 2.0 verbs:

- The **leg setup** command.
- The **aaa authorize** command.

In addition, the following new information tags were added to support the above changes:

- infotag get leg_guid
- infotag get leg_incoming_guid
- infotag get aaa_new_guid

Finally, the following additions were made to the callInfo array:

- CallInfo(guid)

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0538
3690
Doc

- CallInfo(incomingGuid)

Refer to the following *TCL IVR API Command Reference* for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/chapter3.htm

TCL IVR disconnect cause-code Manipulation

The **leg disconnect** command disconnects one or more call legs that are not part of any connection. The cause_code argument, which has been added in Cisco IOS Release 12.2(1)T, is an integer ISDN cause code for the disconnect. It is of the form di-xxx or just xxx, where xxx is the ISDN cause code. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2.htm

TCL-Enabled Signaling Parameter Mapping

The TCL-Enabled Signaling Parameter Mapping feature provides control over call signaling information elements from a Tool Command Language (TCL) Interactive Voice Response (IVR) script to make the Cisco Media-Gateway (that is, the Cisco AS5300 and Cisco AS5800 platforms) interoperable with British Telecom and France Telecom networks. New parameters were introduced under the **set callinfo** command. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/chapter3.htm

TCP Window Scaling

TCP Window Scaling adds support for the Window Scaling extension option in RFC 1323. To improve TCP performance in network paths with a large bandwidth-delay product, Long Fat Networks (LFNs), a larger window size is recommended. This TCP Window Scaling enhancement provides that support.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/tcpwslfn.htm

Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series Routers

The Trimble Palisade Smart Antenna can provide a signal that can by used for NTP time-synchronization of a network. The Trimble Palisade NTP Synchronization Kit can be connected to the auxiliary port of a Cisco 7200 router. The refclock (reference clock) driver provided by this feature provides the ability to receive an RTS time-stamp signal on the auxiliary port of the router.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtrimble.htm

TX Ring Adjustment

Each permanent virtual circuit (PVC) has a hardware transmit queue, or TX ring. It is a simple FIFO queue, and on the c820 it has a default size of 16 packets. This feature allows adjustment of the size of the TX ring. If both voice and data packets are transmitted on the same PVC, the length of the TX ring must be reduced to a value of about 3 packets. This reduces delay and jitter for voice packets by decreasing the maximum number of data packets or fragments that can be in front of a voice packet inside the TX ring.

Using 31-Bit Prefixes on IPv4 Point-to-Point Links

The Using 31-Bit Prefixes on IPv4 Point-to-Point Links feature allows 31-bit prefixes to be used on IP version 4 point-to-point links. The number of IP addresses is reduced by 50 percent and the number of denial of service (DoS) attacks is also reduced. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft31addr.htm

Virtual Circuit (VC) Merge

The Virtual Circuit (VC) Merge feature allows multiple incoming VCs to be merged into a single outgoing VC. The feature is only available on frame-based connections carrying ATM Adaptation Layer 5 (AAL5) frames consisting of multiple cells. VC Merge helps scale Multiprotocol Label Switching (MPLS) networks, because it allocates only one VC to each destination on a link.

RCS nº 03/2005 - CN
CPMI - CORREIOS
0539
Fls. Nº
3690
Doc.

14246
A-

VC merge maps several incoming labels to one single outgoing label. Cells from different virtual channel identifiers (VCIs) traveling to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections.

VC merge allows the switch to transmit cells coming from different VCIs over the same outgoing VCI to the same destination. In other words, VC merge queues AAL5 frames in input buffers until the switch receives the last frame. Then the switch transmits the cells from that AAL5 frame before it sends any cells from other frames. VC merge requires the switch to provide buffering, but no more buffering than is required in IP networks. VC merge slightly delays the transfer of frames; however, VC merge is for IP traffic and not for traffic that requires speed. IP traffic tolerates delays better than other traffic on the ATM network.

VoAAL2 Profile 9 Support for BLES Interoperability

This feature allows Cisco routers to provide VoAAL2 (Voice over ATM Adaption Layer 2) Profile 9 (G.711ulaw and G.711alaw with 44-byte voice payload) for interoperability with V5.2 and GR.303 Voice GW to Class 5 switches. This feature allows service providers to deliver voice services over xDSL and T1 ATM networks from Class 5 switches.

V... Application Access To SS7 Signaling

The Voice Application Access To SS7 Signaling feature provides a means of transporting ISUP signaling messages from SS7 networks to VoIP networks. ISUP messages and parameters are converted to Generic Transparency Descriptor (GTD) format and transported by the underlying call signalling messages to each node transited by the call.

Refer to the following document for information about the information tags that are associated with this feature:

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/chapter4.htm

Voice over IP Q.SIG Network Transparency

Integration of Q.SIG with the Cisco AS5400 universal access server enables Cisco voice switching services to connect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) that communicate by using the Q.SIG protocol.

The Q.SIG protocol is a variant of ISDN D-channel voice signaling. It is based on the ISDN Q.921 and Q.931 standards and is becoming a worldwide standard for PBX interconnection. By using Q.SIG signaling, the Cisco AS5300 can route incoming voice calls from a private integrated services network exchange (PINX) across a wide-area network (WAN) to a peer Cisco AS5400, which can then transport the signaling and voice packets to a second PINX.

Q.SIG on the AS5400 allows the user to place Q.SIG calls into and receive Q.SIG calls from Cisco Voice-over-IP (VoIP) networks. The Cisco packet network appears to PBXs as a large, distributed transit PBX that can establish calls to any destination served by a Cisco voice node. The switched voice connections are established and torn down in response to Q.SIG control messages that come over an ISDN PRI D channel. The Q.SIG message is passed transparently across the IP network and the message appears to the attached PINXs as a transit network. The PINXs are responsible for processing and provisioning the attached services.

Note This feature was originally introduced in Cisco IOS Release 12.0(7)T on the Cisco AS5300 platform. This release ports the feature into the Cisco AS5400 platform.

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0540
Doc. 3690

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 55.

Table 55 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Important Notes

The following sections contain important notes about Cisco IOS Release 12.3.

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.
- Product Bulletins—If you have an account on Cisco.com, you can find Product Bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find Product Bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0541
Doc. 3690

- *What's Hot for IOS Releases: Cisco IOS 12.3—What's Hot for IOS Releases: Cisco IOS 12.3* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.3. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases: Cisco IOS 12.3* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center**: **Cisco IOS Software**: **What's Hot for IOS Releases**.
- *What's New for IOS—What's New for IOS* lists Cisco IOS software releases that have been recently posted and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center**: **Cisco IOS Software**: **What's New for IOS**.

Important Notes for Cisco IOS Release 12.3(1)

The following information applies to Cisco IOS Release 12.3(1)

Cisco Images Deferred Because of Caveat CSCeb31735

Five images in Cisco IOS Release 12.3(1) were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCeb31735. This caveat affects the following images:

- rpm-boot-mz
- rpm-jk9o3s-mz
- rpm-js-mz
- rpmxf-boot-mz
- rpmxf-p12-mz

With caveat CSCeb31735, this DDTS is used to track the deferral of unsupported RPM and RPM-XF images that are listed above. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco IOS Packaging

Cisco IOS Packaging redefines and simplifies the current Cisco IOS software feature sets. Cisco greatly improves the customer software selection experience by reducing the number of packages from forty-four to eight. The first four packages have been designed to satisfy requirements in four typical service categories: IP data, converged voice and data, Security and VPN, and Enterprise routing protocols. Three additional premium packages offer new Cisco IOS software feature combinations that address more complex network requirements. All features merge in the most premium package, Advanced Enterprise Services, which integrates support for all routing protocols with voice, Security and VPN capabilities.

Doc. 3690

JU.240
A.

Feature inheritance is another powerful aspect of Cisco IOS Packaging. Once a feature is introduced, it is not removed in the more comprehensive packages. Feature inheritance principle provides clear migration, clarifying the feature content of the different packages and how they relate to one another.

Cisco IOS Packaging also simplifies image naming. Each name has been designed to effectively convey the high-level feature content of, and the inheritance characteristics for, the new packages.

Cisco IOS Packaging will be available for customers in Cisco IOS software major release 12.3. It will be supported on the Cisco 1700, Cisco 2600, and Cisco 3700 series routers. Most Cisco Access, Aggregation, and Core routers will support this model in the future.

For additional information about Cisco IOS Packaging, refer to the following product bulletin:

http://www.cisco.com/warp/public/732/releases/packaging/docs/pb.pdf

Caveats for Cisco IOS Release 12.3

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

For information on caveats in Cisco IOS Release 12.3, refer to the *Caveats for Cisco IOS Release 12.3* document, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3 and is located on Cisco.com and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support**: **Software Center**: **Cisco IOS Software**: **BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0543
3690
Doc:

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – MANUAL VOLUME III

2003
PASTA 25

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0544
Doc. 3690

15.322
A

Manual 10

IBM Tivoli
Storage Area Network Manager
Guia do Planejamento e Instalação
Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0545
Doc. 3690

15.321

IBM Tivoli Storage Area Network Manager

Guia de Planejamento e Instalação

Versão 1 Release 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
0546
Fls. Nº
Doc. 3690

S517-7575-01

15.320
A.

Prefácio

O IBM Tivoli Storage Area Network Manager gerencia todos os seus dispositivos em uma SAN (Rede de Área de Armazenamento). As capacidades incluem discovery, monitoração, disponibilidade e gerenciamento de eventos. O *IBM Tivoli Storage Area Network Manager: Guia do Usuário* descreve como gerenciar os recursos na rede de área de armazenamento.

Este manual fornece informações para ajudá-lo a desempenhar as seguintes tarefas:

- Planejar a instalação do IBM Tivoli Storage Area Network Manager
- Instalar o IBM Tivoli Storage Area Network Manager
- Configurar o IBM Tivoli Storage Area Network Manager

Quem Deve Ler Este Guia

Este manual inclui instruções para que instaladores e administradores de SAN planejem, instalem e configurem o IBM Tivoli Storage Area Network Manager. Esses instaladores e administradores devem estar familiarizados com o seguinte:

- Procedimentos gerais para a instalação de softwares em um sistema Windows
- Conceitos da SAN
- DB 2 (Database 2)
- Conceitos de SNMP (Simple Network Management Protocol)
- Tivoli NetView

Depois de instalar o IBM Tivoli Storage Area Network Manager, você deve ler o *IBM Tivoli Storage Area Network Manager: Manual do Usuário*. Ele o ajudará a obter noções básicas sobre o uso do produto.

Publicações

Esta seção lista as publicações na biblioteca do IBM Tivoli Storage Area Network Manager e quaisquer outros documentos relacionados. Também descreve como acessar publicações Tivoli on-line, como solicitar solicitar essas publicações Tivoli e como fazer comentários sobre elas.

Publicações do IBM Tivoli Storage Area Network Manager

A tabela a seguir lista as publicações do IBM Tivoli Storage Area Network Manager.

Título da Publicação	Número de Ordem
IBM Tivoli Storage Area Network Manager: Guia do Usuário	S517-7576
IBM Tivoli Storage Area Network Manager Planning and Installation Guide	SC23-4697
IBM Tivoli Storage Area Network Manager Messages	SC32-0953

A biblioteca do Tivoli Storage Area Network Manager em todos os idiomas está disponível no seguinte CD:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0547
3690
Doc.

© Copyright IBM Corp. 2002, 2003

- Reúnem informações ao nível do host, como sistemas de arquivos e mapeamento para LUNs (Unidades lógicas).
- Reúnem informações sobre o evento e outras informações detectadas pelos HBAs (Adaptadores de Barramento do Host).

15.319
A.

Gerenciamento da Rede da Área de Armazenamento

O gerenciamento da SAN descobre automaticamente os componentes e dispositivos da SAN, além da topologia do ambiente de rede de área de armazenamento. É possível monitorar a utilização do armazenamento na SAN e determinar a disponibilidade dos componentes da SAN.

Descoberta

O processo de localização de recursos dentro de uma empresa, incluindo a detecção da topologia da rede, é chamada de *descoberta*. Os dados coletados são armazenados no banco de dados do Tivoli Storage Area Network Manager. O Tivoli Storage Area Network Manager utiliza os dois métodos a seguir para descobrir sua rede:

Na banda
O agente em cada host gerenciado coleta informações sobre o próprio sistema host, incluindo informações sobre sistema de arquivos. Os comandos são enviados por meio das placas HBA que conectam o sistema host à SAN para reunir informações sobre os dispositivos.

Fora da banda
O gerenciador também pode utilizar consultas do SNMP para descobrir informações sobre comutadores da estrutura selecionados. As informações sobre MIB (Management Information Base) são coletadas a partir desses comutadores.

Uma descoberta é acionada por estes eventos:

- Um usuário solicita uma descoberta (executar poll agora).
- Ocorre um evento que faz com que o IBM Tivoli Storage Area Network Manager execute uma descoberta.
- Uma descoberta planejada ou periódica é iniciada. Uma descoberta planejada se torna padrão a cada 24 horas.
- Um host gerenciado ou um agente SNMP foi incluído.

A Tabela 1 explica quando é executada uma descoberta completa e uma descoberta de topologia.

Tabela 1.

Tipos de Descoberta	Uma Descoberta É Executada Quando:
Completa Dependendo do número de objetos a descobrir, uma descoberta completa pode levar muito tempo para concluir. É possível especificar quando executar uma descoberta completa.	• Um usuário pede uma descoberta (poll agora) • Uma descoberta planejada ou periódica é iniciada • Um host gerenciado é adicionado

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0548
Doc. 3690

Descoberta de SCSI na Internet

O Tivoli Storage Area Network Manager também suporta a descoberta de iSCSI (Internet SCSI). A descoberta de iSCSI é executada independentemente da descoberta feita pelo Tivoli Storage Area Network Manager e exige que você ative a descoberta de IP do Tivoli NetView. Para obter informações adicionais, consulte "Suporte à Internet SCSI" na página 5.

Exibições da Topologia

O Tivoli Storage Area Network Manager extrai informações sobre estrutura a partir do banco de dados e utiliza o Tivoli NetView para exibir a topologia da estrutura. A Tabela 2 descreve as exibições disponíveis para as SANs. Para cada dispositivo descoberto e exibido, é possível abrir um diálogo de propriedades que mostra os atributos e as conexões associados a esse dispositivo.

Tabela 2. Descrição das Exibições da SAN a partir do Tivoli NetView

Exibições da SAN	Descrição
Símbolos da SAN (do Submapa Raiz)	Exibe um símbolo para cada SAN. Dê um clique duplo em um símbolo da SAN para exibir o seu submapa. A partir de um submapa você pode optar por uma das seguintes exibições: • Exibição de Topologia: Exibe a SAN inteira com dois tipos de símbolos, um para os elementos da conexão da SAN e outro para cada segmento da estrutura. • Exibição em Zonas: Exibe a SAN como um agrupamento de zonas.
Centrada no host	Exibe todos os sistemas host e suas relações lógicas com dispositivos locais e conectados à SAN. Não exibe os comutadores e outros dispositivos de conexão.
Centrada no dispositivo	Exibe todos os dispositivos de armazenamento e suas relações lógicas com todos os hosts. Não exibe os comutadores e outros dispositivos de conexão.

Eventos do SNMP

O IBM Tivoli Storage Area Network Manager pode enviar eventos, que representam uma alteração no estado da estrutura, para qualquer console do evento dentro da empresa do qual o IBM Tivoli Storage Area Network Manager participa. Esses eventos são gerados nos formatos SNMP e Tivoli Enterprise Console.

Detecção de Erros e Isolamento de Falhas

A função EDFI (Detecção de Erros e Isolamento de Falhas) ajuda na determinação de problemas em links de interconexão SAN Fibre Channel. A EDFI identifica o hardware com defeito utilizando uma técnica de análise de falhas previstas com base na modelagem estatística das distribuições da falha do componente. A EDFI procura os dados de erros temporários pela SAN e analisa-os quanto a padrões. O hardware ótico e elétrico muitas vezes falha de forma tal que condições intermitentes podem ser identificadas antes que se tornem uma falha permanente. Além disso, o isolamento de falhas é feito para isolar o componente avariado. O objetivo é identificar a ótica com falha e os componentes de interconexão e notificar os usuários antes que realmente ocorra uma falha de hardware. É importante que essa notificação seja resolvida rapidamente. O componente com as taxas de erros temporários elevadas deve ser substituído antes que se torne realmente uma falha permanente. A EDFI não analisa erros para componentes

15.318
RQS nº 03/2005 - CN
CORREIOS
Fls. Nº 0549
Doc. 3690

Os agentes SNMP utilizam protocolos de descoberta fora de banda que, por sua vez, utilizam consultas SNMP em uma conexão TCP/IP para reunir informações sobre topologia e atributos. Para incluir um agente SNMP, siga estas etapas:

1. Clique em **Incluir**.
2. A caixa de diálogo Inserir Endereço IP é exibida. Insira um nome ou endereço IP e clique em **OK**.
3. O agente SNMP é incluído na lista de agentes SNMP. O estado desse agente deve ser **Contactado**. Clique em **OK**. Se você não visualizar um estado **Contactado**, verifique se o nome ou endereço IP está correto. Em seguida, verifique se o comutador realmente oferece suporte para descoberta fora de banda.

Nota: O botão **Avançado** é válido somente para comutadores Brocade®. Quando você selecionar um agente no painel Configuração de Agentes e clicar no botão **Avançado**, deverá inserir um ID do usuário e uma senha para o comutador Brocade. Será necessário inserir as informações de login para a conta "admin" no Comutador Brocade. Nenhuma outra conta será suportada.

Depois de inserir o ID do usuário e a senha e o próximo poll ser executado, verifique a seguinte mensagem no log de mensagens:

```
The user ID or password entered for the outband agent target
address <target_address> is incorrect.
```

Se você vir essa mensagem, insira novamente o ID do usuário e a senha corretos.

Configurando o Arquivo MIB no Tivoli NetView

Depois de instalar o Tivoli NetView, você precisará criar entradas de trap no arquivo trapd.conf do Tivoli NetView. *Não* edite o arquivo manualmente. A edição é feita por meio de um arquivo em batch criado pelo programa mib2trap do Tivoli NetView. O arquivo ITSANM.mib está localizado no diretório /misc/utils do CD do Tivoli Storage Area Network Manager. Siga estas etapas:

1. Execute o programa mib2trap no arquivo ITSANM.mib. Especifique o nome completo do caminho para um diretório gravável ao criar o arquivo ITSANM.bat. Por exemplo, execute este comando para criar o arquivo bat no diretório tmp:

   ```
   mib2trap c:\tmp\ITSANM.mib c:\tmp\ITSANM.bat
   ```

   É possível especificar qualquer nome desejado para o arquivo bat. O exemplo a seguir cria o arquivo ITSANM.bat.
2. Execute o arquivo ITSANM.bat.
3. Inicie novamente o Tivoli NetView e torne o monitor visível para ver todos os eventos.

Configurando o IBM Tivoli Storage Area Network Manager para Enviar Eventos

O IBM Tivoli Storage Area Network Manager oferece suporte para a monitoração centralizada de eventos em toda a sua empresa. Se você utiliza um sistema como o Tivoli Enterprise Console ou um aplicativo capaz de receber eventos SNMP, o IBM Tivoli Storage Area Network Manager pode ser facilmente configurado para enviar eventos a esse sistema ou aplicativo. Se você não estiver utilizando um aplicativo

15.317 A.
RGSTR 03/2005 - CN
CPMI - CORREIOS
0550
Fls. N
3690
Doc.

15.316
A.

Manual 11

IBM Tivoli Storage Manager for AIX
Administrator`s Guide
Versão 5.2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0551
Doc. 3690

IBM Tivoli Storage Manager
for AIX

15.315

Administrator's Guide

Version 5.2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0652
Doc. 3690

GC32-0768-01

15-314
A.

Chapter 1. Introducing IBM Tivoli Storage Manager

IBM Tivoli Storage Manager is an enterprise-wide storage management application. It provides automated storage management services to workstations, personal computers, and file servers from a variety of vendors, with a variety of operating systems. Tivoli Storage Manager includes the following components:

Server

Server program
The server program provides backup, archive, and space management services to the clients.

You can set up multiple servers in your enterprise network to balance storage, processor, and network resources.

Administrative interface
The administrative interface allows administrators to control and monitor server activities, define management policies for clients, and set up schedules to provide services to clients at regular intervals. Administrative interfaces available include a command-line administrative client and a Web browser interface. Tivoli Storage Manager allows you to manage and control multiple servers from a single interface that runs in a Web browser.

Server database and recovery log
The Tivoli Storage Manager server uses a database to track information about server storage, clients, client data, policy, and schedules. The server uses the recovery log as a scratch pad for the database, recording information about client and server actions while the actions are being performed.

Server storage
The server can write data to hard disk drives, disk arrays and subsystems, stand-alone tape drives, tape libraries, and other forms of random- and sequential-access storage. The media that the server uses are grouped into *storage pools*. The storage devices can be connected directly to the server, or connected via local area network (LAN) or storage area network (SAN).

Client Nodes
A client node can be a workstation, a personal computer, a file server, a network-attached storage (NAS) file server, or even another Tivoli Storage Manager server. The client node has IBM Tivoli Storage Manager client software installed (except for NAS file servers using NDMP). A client node is registered with the server.

Backup-archive client
The backup-archive client allows users to maintain backup versions of files, which they can restore if the original files are lost or damaged. Users can also archive files for long-term storage and retrieve the archived files when necessary. Users themselves or administrators can register workstations and file servers as client nodes with a Tivoli Storage Manager server.

The storage agent is an optional component that may also be installed on a system that is a client node. The storage agent enables LAN-free data movement for client operations and is supported on a number of operating systems.

RQS nº 03/2005 - CN
CORREIOS
0553
3690

© Copyright IBM Corp. 1993, 2003

- Check enough scratch or private volumes into the library to handle the expected load.

- If your clients tend to store files of smaller sizes, controlling the transaction size can affect how WORM platters are used. Smaller transactions waste less space if a transaction such as a backup must be canceled. The TXNGROUPMAX server option and the TXNBYTELIMIT client option control transaction size. See "How the Server Groups Files before Storing" on page 196 for information.

Managing Volumes in Automated Libraries

Tivoli Storage Manager tracks the scratch and private volumes available in an automated library through a *library volume inventory*. Tivoli Storage Manager maintains an inventory for each automated library. The library volume inventory is separate from the inventory of volumes for each storage pool. To add a volume to a library's volume inventory, you *check in* a volume to that Tivoli Storage Manager library. For details on the check-in procedure, see "Checking New Volumes into a Library" on page 137.

To ensure that Tivoli Storage Manager's library volume inventory remains accurate, you must *check out* volumes when you need to physically remove volumes from a SCSI, 349X, or ACSLS library. When you check out a volume that is being used by a storage pool, the volume remains in the storage pool. If Tivoli Storage Manager requires the volume to be mounted while it is checked out, a message to the mount operator's console is displayed with a request to check in the volume. If the check in is not successful, Tivoli Storage Manager marks the volume as unavailable.

While a volume is in the library volume inventory, you can change its status from scratch to private.

To check whether Tivoli Storage Manager's library volume inventory is consistent with the volumes that are physically in the library, you can audit the library. The inventory can become inaccurate if volumes are moved in and out of the library without informing the server via volume check-in or check-out.

Task	Required Privilege Class
Changing the status of a volume in an automated library Removing volumes from a library Returning volumes to a library	System or unrestricted storage

Changing the Status of a Volume

The UPDATE LIBVOLUME command lets you change the status of a volume in an automated library from scratch to private, or private to scratch. However, you cannot change the status of a volume from private to scratch if the volume belongs to a storage pool or is defined in the volume history file. You can use this command if you make a mistake when checking in volumes to the library and assign the volumes the wrong status.

Removing Volumes from a Library

You may want to remove a volume from an automated library. The following two examples illustrate this:

- You have exported data to a volume in the library and want to take it to another system for an import operation.

15.313
J.A.
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0554
Doc. 3690

- All of the volumes in the library are full, and you want to remove some that are not likely to be accessed to make room for new volumes that can be used to store more data.

15.312

To remove a volume from an automated library, use the CHECKOUT LIBVOLUME command. By default, the server mounts the volume being checked out and verifies the internal label. When the label is verified, the server removes the volume from the library volume inventory, and then moves it to the entry/exit port or convenience I/O station. of the library. If the library does not have an entry/exit port, Tivoli Storage Manager requests that the mount operator remove the volume from a slot within the library.

For SCSI libraries with multiple entry/exit ports, use the REMOVE=BULK parameter of the CHECKOUT LIBVOLUME command to eject the volume to the next available entry/exit port.

If you check out a volume that is defined in a storage pool, the server may attempt to access it later to read or write data. If this happens, the server requests that the volume be checked in.

Returning Volumes to a Library

When you check out a volume that is defined to a storage pool, to make the volume available again, do the following:

1. Check in the volume for the library, with private status. Use the CHECKIN LIBVOLUME command with the parameter STATUS=PRIVATE.
2. If the volume was marked unavailable, update the volume's ACCESS value to read/write or read-only. Use the UPDATE VOLUME command with the ACCESS parameter.

Managing a Full Library

As Tivoli Storage Manager fills volumes in a storage pool, the number of volumes needed for the pool may exceed the physical capacity of the library. To make room for new volumes while keeping track of existing volumes, you can define a storage pool overflow location near the library. You then move media to the overflow location as needed. The following shows a typical sequence of steps to manage a full library:

1. Define or update the storage pool associated with the automated library, including the overflow location parameter. For example, you have a storage pool named ARCHIVEPOOL associated with an automated library. Update the storage pool to add an overflow location of Room2948. Enter this command:

   ```
   update stgpool archivepool ovflocation=Room2948
   ```

2. When the library becomes full, move the full volumes out of the library and to the overflow location that you defined for the storage pool. For example, to move all full volumes in the specified storage pool out of the library, enter this command:

   ```
   move media * stgpool=archivepool
   ```

   All full volumes are checked out of the library. Tivoli Storage Manager records the location of the volumes as Room2948. You can use the DAYS parameter to specify the number of days that must elapse before a volume is eligible for processing by the MOVE MEDIA command.
3. Check in new scratch volumes, if needed.
4. Reuse the empty scratch storage volumes in the overflow location. For example, enter this command:

RGSP 03/2005 CN
CPMI - CORREIOS
Fls. Nº 0555
Doc. 3690

Table 15. Task Tips for Storage Pools

For this Goal	Do This	For More Information
Keep the data for a client on as few volumes as possible	Enable collocation for the storage pool	"Keeping a Client's Files Together: Collocation" on page 208
Reduce the number of volume mounts needed to back up multiple clients	Disable collocation for the storage pool	"Keeping a Client's Files Together: Collocation" on page 208
Perform a simultaneous write to a primary storage pool and copy storage pools	Provide a list of copy storage pools when defining the primary storage pool.	"Simultaneous Write to a Primary Storage Pool and Copy Storage Pools"
Specify how the server reuses tapes	Set a reclamation threshold for the storage pool Optional: Identify a reclamation storage pool	"Reclaiming Space in Sequential Access Storage Pools" on page 213
Move data from disk to tape automatically when needed	Set a migration threshold for the storage pool Identify the next storage pool	"Migration for Disk Storage Pools" on page 200
Move data from disk to tape automatically based on how frequently users access the data or how long the data has been in the storage pool	Set a migration threshold for the storage pool Identify the next storage pool Set the migration delay period	"Migration for Disk Storage Pools" on page 200
Back up your storage pools	Define a copy storage pool Set up a backup schedule	"Defining a Copy Storage Pool" on page 244 "Automating a Basic Administrative Command Schedule" on page 401
Have clients back up directly to a tape storage pool	Define a sequential access storage pool that uses a tape device class Change the policy that the clients use, so that the backup copy group points to the tape storage pool as the destination.	"Defining or Updating Primary Storage Pools" on page 182 "Changing Policy" on page 300

Simultaneous Write to a Primary Storage Pool and Copy Storage Pools

To simultaneously write data to a primary storage pool and one or more copy storage pools, you can specify a list of copy storage pools in a primary storage pool definition using the COPYSTGPOOLS parameter. When a client backs up, archives, or migrates a file, the file is written to the primary storage pool and is simultaneously stored into each copy storage pool. If a write failure occurs for any of the copy storage pools, the COPYCONTINUE parameter setting determines how the server should react. See Table 14 on page 183 for additional information about storage pool definitions.

When using copy storage pools for the simultaneous write of data to a primary storage pool and associated copy storage pools, be sure that enough resources, such as drives, are available for the write operation. For example, each simultaneous write operation will need all of the volumes to be simultaneously mounted. This requires that the number of available drives must be equal to or

ROS nº 03/2005 - CN
CPMI - CORREIOS
0556
Fls. Nº
Doc. 3690

TAPEPOOL
The next storage pool in the hierarchy. It contains tape volumes accessed by high-performance tape drives.

15.310

Assume a user wants to archive a 5MB file that is named *FileX*. FileX is bound to a management class that contains an archive copy group whose storage destination is DISKPOOL, see Figure 19 on page 197.

When the user archives the file, the server determines where to store the file based on the following process:

1. The server selects DISKPOOL because it is the storage destination specified in the archive copy group.
2. Because the access mode for DISKPOOL is read/write, the server checks the maximum file size allowed in the storage pool.

   The maximum file size applies to the physical file being stored, which may be a single client file or an aggregate. The maximum file size allowed in DISKPOOL is 3MB. FileX is a 5MB file and therefore cannot be stored in DISKPOOL.
3. The server searches for the next storage pool in the storage hierarchy.

   If the DISKPOOL storage pool has no maximum file size specified, the server checks for enough space in the pool to store the physical file. If there is not enough space for the physical file, the server uses the next storage pool in the storage hierarchy to store the file.
4. The server checks the access mode of TAPEPOOL, which is the next storage pool in the storage hierarchy. The access mode for TAPEPOOL is read/write.
5. The server then checks the maximum file size allowed in the TAPEPOOL storage pool. Because TAPEPOOL is the last storage pool in the storage hierarchy, no maximum file size is specified. Therefore, if there is available space in TAPEPOOL, FileX can be stored in it.

Using Copy Storage Pools to Back Up a Storage Hierarchy

Copy storage pools enable you to back up your primary storage pools for an additional level of data protection for clients. See "Backing Up Storage Pools" on page 549 for details. Copy storage pools are not part of a storage hierarchy.

For efficiency, it is recommended that you use one copy storage pool to back up all primary storage pools that are linked to form a storage hierarchy. By backing up all primary storage pools to one copy storage pool, you do not need to recopy a file when the file migrates from its original primary storage pool to another primary storage pool in the storage hierarchy.

When defining copy storage pools to primary pools that have defined next pools, the copy pool list for each primary pool should be the same. Defining different copy pool lists can cause resources to be freed when failing over to the next pool. If the resources are freed, it can delay the completion of client operations.

In most cases, a single copy storage pool can be used for backup of all primary storage pools. The number of copy storage pools you need depends on whether you have more than one primary storage pool hierarchy and on what type of disaster recovery protection you want to implement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0557
3690
Doc.

Multiple copy storage pools may be needed to handle particular situations, including:

15.309
4-

Manual 12

IBM Tivoli Storage Manager for Database Version 5.2 Data Protection for Oracle for UNIX Installation and User`s Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0558
3690
Doc.

15.303
A-

IBM Tivoli Storage Manager for Databases Version 5.2

Data Protection for Oracle for UNIX Installation and User's Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
0559
Fls. Nº
Doc. 3690

SC32-9064-00

15.307
A.

Preface

IBM Tivoli Storage Manager for Databases Version 5.2 Data Protection for Oracle is referred to as *Data Protection for Oracle* throughout this book.

Data Protection for Oracle performs online or offline backups of Oracle8i or Oracle9i databases to Tivoli Storage Manager storage. This integration with the RMAN Media Management API maximizes the protection of data, thus providing a comprehensive storage management solution.

Tivoli Storage Manager is a separate client-server licensed product that provides storage management services in a multi-platform computer environment.

Who should read this publication

The target audience for this publication are system installers, system users, Oracle database administrators, and system administrators .

In this book, it is assumed that you have an understanding of the following applications:

- Oracle Server
- Tivoli Storage Manager Server
- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager Application Program Interface

It is also assumed that you have an understanding of one of the following operating systems:

- AIX
- HP-UX
- Linux
- Solaris Operating Environment (hereinafter referred to as Solaris)

IBM Tivoli Storage Manager Web site

Technical support information and publications are available at the following address:

`www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html`

By accessing the Tivoli Storage Manager home page, you can access subjects that interest you. You can also keep up-to-date with the newest Tivoli Storage Manager product information.

IBM Tivoli Storage Manager publications

Table 1. Related Tivoli Storage Manager publications

Title	Order Number
IBM Tivoli Storage Manager for Windows Backup-Archive Client Installation and User's Guide	GC32-0788
IBM Tivoli Storage Manager for UNIX Backup-Archive Clients Installation and User's Guide	GC32-0789

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0560
3690
Doc.

© Copyright IBM Corp. 1997, 2003

15.306
A.

Manual 13

IBM Tivoli Storage Manager for Mail 5.1.5 Data Protection for Microsoft Exchange Server Installation and User`s Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
0561
Fls. Nº
3690
Doc.

15.305
A.

IBM Tivoli Storage Manager for Mail 5.1.5

Data Protection for Microsoft Exchange Server Installation and User's Guide

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0562
3690
Doc.

SC32-9058-00

15.304
A.

Preface

IBM Tivoli Storage Manager for Mail 5.1.5 Data Protection for Microsoft Exchange Server is referred to as *Data Protection for Exchange* throughout this book.

Tivoli Storage Manager and *Tivoli Storage Manager Server* are referred to as *Storage Manager* and *Storage Manager Server* respectively throughout this book.

Data Protection for Exchange performs online backups of Microsoft Exchange Server databases to Tivoli Storage Manager storage. This integration with the Microsoft Exchange Server application program interface (API) maximizes the protection of data, thus providing a comprehensive storage management solution.

Storage Manager is a separate client-server licensed product that provides storage management services in a multi-platform computer environment.

Who should read this book

The target audience for this book are system installers, system users, and system administrators.

In this book, it is assumed that you have an understanding of the following applications:

Microsoft Exchange Server

Storage Manager Server

Storage Manager Backup-Archive Client

Storage Manager Application Program Interface

It is also assumed that you have an understanding of one of the following operating systems:

- Windows NT
- Windows 2000

Throughout this document, the term Windows refers to both Windows NT Server and Windows 2000 Server.

What this book contains

The book contains the following sections:

- Chapter 1, "Introducing Data Protection for Exchange" on page 1

  This section provides an overview of Data Protection for Exchange.
- Chapter 2, "Installing Data Protection for Exchange" on page 9

  This section explains the environment requirements and steps necessary to install Data Protection for Exchange.
- Chapter 3, "Configuring Data Protection for Exchange" on page 13

  This section explains registering and configuring Data Protection for Exchange and provides policy recommendations.
- Chapter 4, "Using the Graphical User Interface (GUI)" on page 49

  This section explains how to perform Data Protection for Exchange functions from a graphical user interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0563
Fls. Nº
3690
Doc.

© Copyright IBM Corp. 1998, 2002

15-303
A

Switch Tipo 1 doc1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0564
Doc. 3690

Cisco Systems

15.302
A.

Data Sheet

Cisco Catalyst **6500** Series Switch

The Catalyst 6500 Series sets the new standard for IP communications and application delivery in enterprise campus and service provider networks by maximizing user productivity and enhancing operational control while providing unprecedented investment protection. As Cisco's premier intelligent multilayer modular switch, the Catalyst® 6500 Series delivers secure, converged services, end-to-end, from the wiring closet to the core, to the data center, to the WAN edge.

Ideal for enterprises and service providers seeking to reduce their total cost of ownership, the Cisco Catalyst 6500 Series delivers scalable performance and port density across a range of chassis configurations and LAN/WAN/MAN interfaces. Available in 3-, 6-, 9-, and 13-slot chassis, Cisco Catalyst 6500 Series switches feature an unparalleled range of integrated services modules, including multigigabit network security, content switching, telephony, and network analysis modules.

By taking advantage of a forward-thinking architecture that uses a common set of modules and operating system software across all Cisco Catalyst 6500 Series chassis, the Catalyst 6500 Series delivers a high level of operational consistency that optimizes IT infrastructure usage and enhances return on investment. From 48-port to 576-port 10/100/1000 Ethernet wiring closets to hundreds-of-Mpps network cores supporting up to 192 1-Gbps or 32 10-Gbps trunks, the Cisco Catalyst 6500 Series provides an optimal platform that maximizes network uptime with stateful failover capability between redundant routing and forwarding engines.

With numerous industry-firsts and industry-leading features to its credit, the Catalyst 6500 Series supports three generations of modules that continue to demonstrate the Catalyst 6500 value and Cisco's commitment to innovation. Cisco's new generation of Catalyst 6500 Series modules and Supervisor Engine 720 incorporate 11 new Cisco-developed application specific integrated circuits (ASICs)—extending Cisco's leadership in networking while providing unparalleled investment protection.

Figure 1
Cisco Catalyst 6500 Series Chassis

RQS nº 03/2005 - CN
CPMI - CORREIOS
0565
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-301
A-

Cisco Catalyst 6500 Series Benefits

The Cisco Catalyst 6500 Series provides market-leading services, performance, port densities, and availability with investment protection for enterprise and service provider markets. These include:

- *Maximum network uptime*—With platform, power supply, supervisor engine, switch fabric, and integrated network services redundancy provides one- to three-second stateful failover and delivers application and services continuity in a converged network environment, minimizing disruption of mission-critical data and services
- *Comprehensive network security*—Integrates proven, multigigabit Cisco security solutions, including intrusion detection, firewall, VPN, and SSL into existing networks
- *Scalable performance*—Provides up to 400 Mpps performance with distributed forwarding architecture
- *Forward-Thinking architecture with investment protection*—Supports three generations of interchangeable, hot-swappable modules in the same chassis, optimizing IT infrastructure usage, maximizing return on investment, and reducing total cost of ownership
- *Operational consistency*—Features 3-, 6-, 9-, and 13-slot chassis configurations sharing a common set of modules, Cisco IOS Software, Cisco Catalyst Operating System Software, and network management tools that can be deployed anywhere in the network
- *Unparalleled services integration and flexibility*—Integrates advanced services such as security and content with converged networks, provides the widest range of interfaces and densities, from 10/100 and 10/100/1000 Ethernet to 10 Gigabit and from DS0 to OC-48, and performs in any deployment end to end

Operational Consistency in End-to-End Cisco Catalyst 6500 Series Deployments

- Features 3-, 6-, 9-, and 13-slot chassis configurations that share a common set of modules, software, and network management tools
- Deploys anywhere in the network—from the wiring closet to the core, to the data center, to the WAN edge
- Shares WAN port adapters with Cisco 7xxx router Series for reduced sparing and training costs
- Offers choice of Cisco IOS Software and Cisco Catalyst Operating System Software supported on all supervisor engines, providing smooth migration from Cisco Catalyst 5000 Series and Cisco 7500 Series deployments

Maximum Network Uptime and Network Resiliency

- Provides packet-loss protection and the fastest recovery from network disruption
- Features fast, one- to three-second stateful failover between redundant supervisor engines
- Offers optional, redundant high-performance Cisco Catalyst 6500 Series Supervisor Engine 720, passive backplane, multimodule Cisco EtherChannel® technology, IEEE 802.3ad link aggregation, IEEE 802.1s/w, and Hot Standby Router Protocol/Virtual Router Redundancy Protocol (HSRP/VRRP) high-availability features

Integrated High-performance Security and Network Management

Integrated gigabit-per-second services modules, deployed where external devices would not be feasible, simplify network management and reduce total cost of ownership. These include:

- Gigabit firewall—provides access protection
- High-performance intrusion detection system (IDS)—provides intrusion detection protection
- Gigabit Network Analysis Module—provides a more manageable infrastructure and full Remote Monitoring (RMON) support
- High-performance SSL—provides high-performance, secure e-commerce traffic termination
- Gigabit VPN and standards-based IP Security (IPSec)—support lower cost Internet and Extranet connections

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0566
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-300
A-

Content-and Application-Aware Layers 2 Through 7 Switching Services

- Integrated content switching module (CSM) brings high-performance, feature-rich server and firewall load balancing to the Cisco Catalyst 6500 Series, ensuring a safer and more manageable infrastructure with unprecedented control
- Integrated multigigabit SSL acceleration combined with CSM provides a high-performance e-commerce solution
- Integrated multigigabit firewall and CSM provide a secure, high-performance, data-center solution
- Software features such as Network Based Application Recognition (NBAR) enhance network management and control of bandwidth utilization

Scalable Performance

- Delivers the industry's highest LAN switch performance, 400 Mpps, using the distributed Cisco Express Forwarding dCEF720 platform
- Supports a mix of Cisco Express Forwarding (CEF) implementations and switch fabric speeds for optimal wiring closet, core, data center, and WAN edge deployments, as well as service provider networks

Rich Layer 3 Services

- Multiprotocol Layer 3 routing supports traditional network requirements and provides a smooth transition mechanism in the enterprise
- Provides hardware support for enterprise-class and service-provider-scale routing tables
- Provides IPv6 support in hardware (using Supervisor Engine 720) with an unparalleled high-performance suite of services
- Provides hardware support for large enterprise-class and service-provider-scale routing tables
- Provides MPLS support in hardware to enable VPN services within the enterprise and facilitate smooth integration with new high-speed service provider core infrastructures and Metro Ethernet deployments

Enhanced Data Voice, and Video Services

- Provides integrated IP communications throughout all Cisco Catalyst 6500 Series platforms
- Provides 10/100 and 10/100/1000 line cards, field upgradable with inline power using a daughter card and offering future support for IEEE 802.3af to protect today's investments
- Provides dense T1/E1 and foreign Exchange Station (FXS) voice-over-IP (VoIP) gateway interfaces for public switched telephone network (PSTN) access and traditional phone, fax, and private branch exchange (PBX) connections
- Supports high-performance IP multicast video and audio applications
- Provides integrated management necessary to effectively deploy a scalable enterprise-converged network

Highest Level of Interface Flexibility, Scalability, and Density

- Provides the port densities and interface choices that large mission-critical wiring closets, enterprise core, and distribution networks require
- Supports up to 576 voice 10/100/1000 Gigabit-over-copper ports with inline power per system
- Provides up to 192 Gigabit Ethernet ports

ROS-A 03/2005 - CN
CPMI CORREIOS
0567
Fls. Nº
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.299
A.

- Features the industry's first 10 Gigabit Ethernet, Channelized OC-48 dense OC-3 Packet over Synchronous Optical Network (SONET) (PoS)
- Provides investment protection by using Cisco 7xxx Series port adapters on the Cisco Catalyst 6500 Series FlexWAN Line Card, supporting T1/E1 through OC-48 WAN interfaces
- Chassis sizes range from 3-slot (Cisco Catalyst 6503 Switch) to 13-slot (Cisco Catalyst 6513 Switch)

High-Speed WAN Interfaces

- Provides high-speed WAN, ATM, and SONET interfaces compatible with other core routers
- Provides single-device management for WAN aggregation and for campus and metro connectivity

Maximum Investment Protection

- Highly flexible modular architecture supports multiple generations of modules that are fully interoperable with each other in the same chassis
- Upgradable supervisor engines can add Layer 3 routing or forwarding capabilities over time
- Cisco IOS Software and Cisco Catalyst Operating System Software are supported across all supervisor engines
- Field-upgradable inline power for 10/100 Mbps and 10/100/1000 Mbps Ethernet modules for "pay as you go" IP telephony and wireless computing
- A steady stream of new services modules adds to the deployment options
- Includes Cisco Catalyst 6500 Series network security, content switching, and voice capabilities
- Future modules will increase performance, port density, and include additional services

Ideal for Metro Ethernet WAN Services

- 802.1Q and 802.1Q tunneling (QinQ) providing point-to-point and multipoint Ethernet services
- EoMPLS in MPLS backbones for superior network scaling providing virtual LAN (VLAN) translation capability
- Layer 2 and Layer 3 QoS enables tiered Ethernet service offerings through rate limiting and traffic shaping
- Superior high-availability features include enhanced Spanning Tree Protocol, IEEE 802.1s, IEEE 802.1w, and Cisco EtherChannel IEEE 802.3ad link aggregation

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
System Feature	
Chassis Configurations	3-slot 6-slot 9-slot 9 vertical slots 13-slot
Backplane Bandwidth	32Gbps shared bus 256Gbps switch fabric 720Gbps switch fabric
L3 Forwarding Performance	Supervisor 1 MSFC: 15 Mpps Supervisor 2 MSFC: up to 210 Mpps Supervisor 720: up to 400 Mpps

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0568
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.298
A-

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
Operating System	Catalyst OS (CatOS) Cisco IOS CatOS/IOS Hybrid Configuration
Redundant Supervisors	Yes, with stateful failover
Redundant Components	Power supplies (1+1) Switch fabric (1+1) Replaceable clock Replaceable fan tray
High Availability Features	Gateway Load Balancing Protocol Hot Standby Router Protocol Multimodule EtherChannel Rapid Spanning Tree Multiple Spanning Tree Per VLAN Rapid Spanning Tree Rapid Convergence L3 Protocols
Maximum System Port Densities	
10/100/1000 Ethernet	576 ports, all support Inline Power
10/100 Fast Ethernet	576 ports, all support Inline Power
100-Base-FX	288 ports
Gigabit Ethernet (GBIC)	194 ports (2 ports provided on supervisor engine)
10 Gigabit Ethernet (XENPAK)	32 ports
Integrated WAN Modules	
FlexWAN (DS0 to OC-3)	12 modules with 24 port adapters
OC-3 POS ports	192
OC-12 POS ports	48
OC-12 ATM ports	24
OC-48 POS/DPT ports	24
PSTN Interfaces	
Digital T1/E1 Trunk ports	216
FXS Interfaces	864
Advanced Services Modules	Gigabit Firewall Gigabit VPN High Performance Intrusion Detection Gigabit Content Switching Module High Performance SSL Termination Gigabit Content Services Gateway

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0569
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

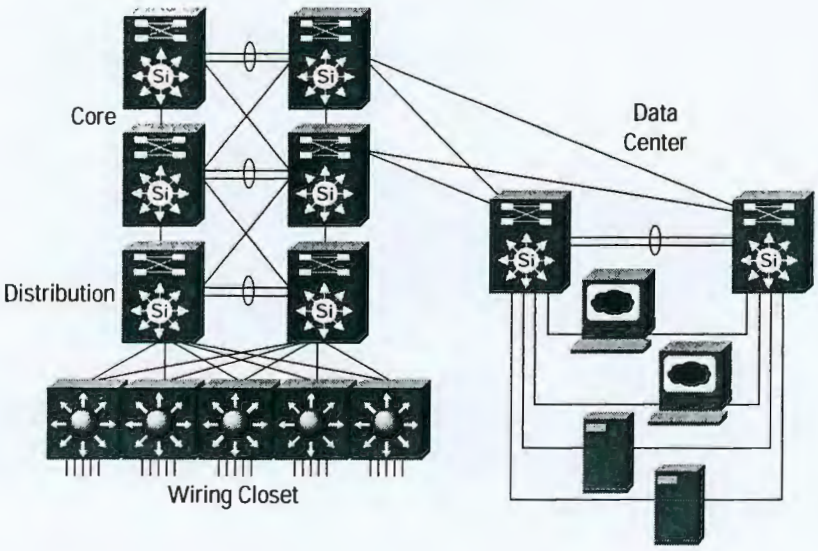
15.297
A-

Deployment Scenarios

The Cisco Catalyst 6500 Series delivers secure converged services for campus, Internet service provider (ISP), metro edge, and research and grid computing networks.

- *Campus networks*—Features 10/100 and 10/100/1000 autosensing modules that provide inline power for the wiring closet, along with robust high availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the distribution and core

Figure 2
Deployment Scenarios for Catalyst 6500 Series Switches in Campus Networks



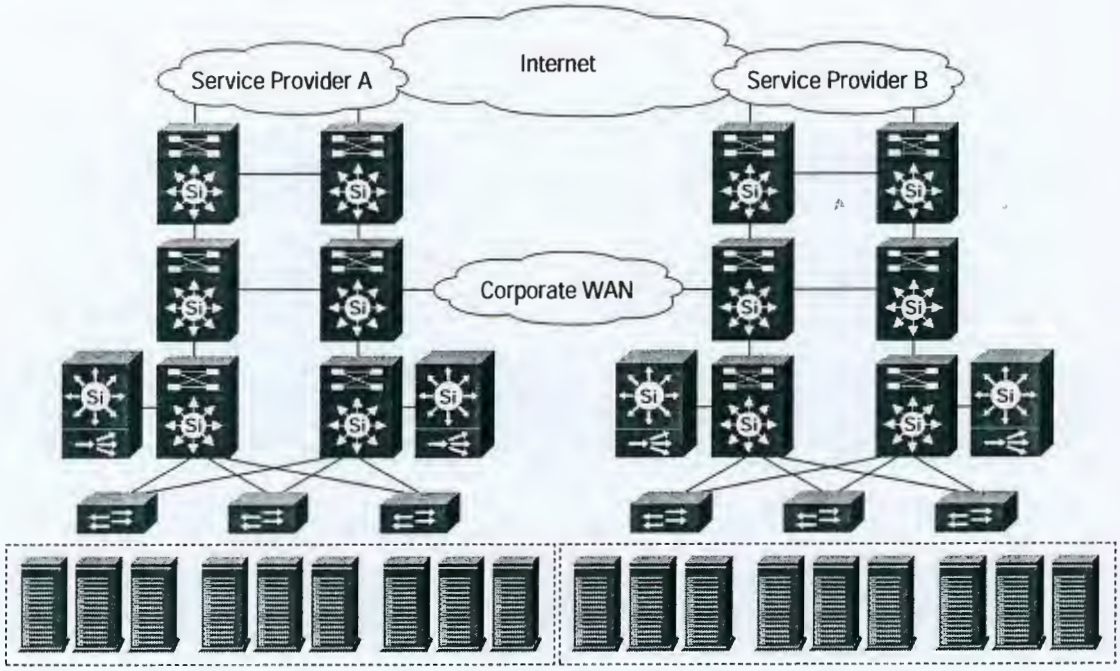
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0570
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.296
A.

- [*ISP network*—Provides robust high-availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the most demanding service provider networking environments requiring Multiprotocol Label Switching (MPLS), Multicast, IP Version 6 (IPv6), an extensive set of WAN interfaces, and hierarchical traffic shaping.

Figure 3
Deployment Scenarios for Catalyst 6500 Series Switches in ISP Networks



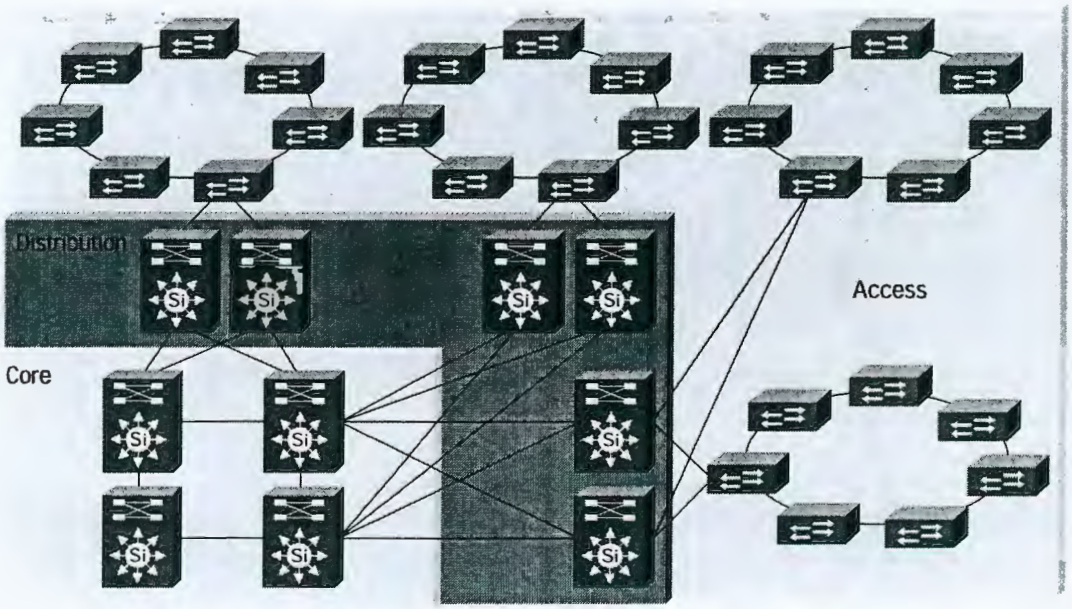
ROS nº 03/2005 - CN
CPMI - CORREIOS
0571
Fls. Nº
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.295
A-

- *Metro edge*—Features edge-, distribution-, and core-layer interfaces for point-to-point and multipoint Ethernet services for metro and inter-metro network deployments with the following features:
  - High-performance 10-Gigabit Ethernet uplinks
  - 802.1Q tunneling
  - Ethernet over MPLS (EoMPLS)
  - Layer 2 and Layer 3 QoS
  - Network Equipment Building Standards (NEBS) compliance
  - Security, high availability, and manageability

Figure 4
Deployment Scenarios for Catalyst 6500 Series Switches in Metro Edge



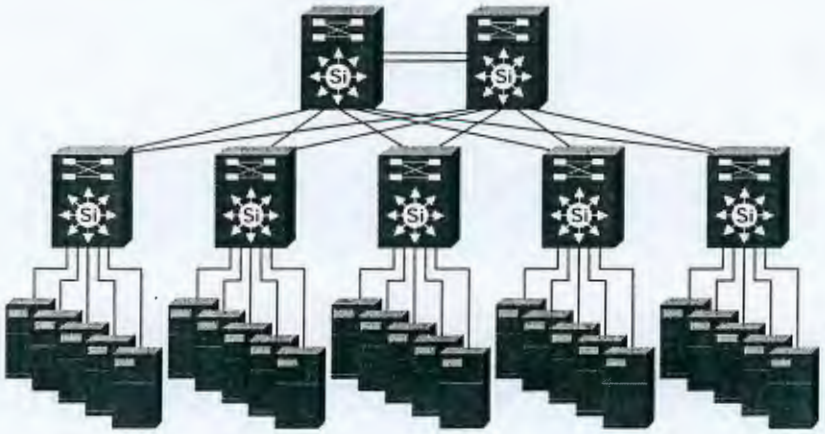
RQS nº 03/2005 - CN
CPMI - CORREIOS
0572
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.294
A.

- *Grid computing network*—Provides high-speed optical interface modules and world-class software required to handle high-volume traffic and build and manage large-scale networks

Figure 5
Deployment Scenarios for Catalyst 6500 Series Switches in Grid Computing Network



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0573
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.293
A.

System Overview

Modular Architecture

The Cisco Catalyst 6500 Series is a modular system that can grow as customer requirements expand and technology evolves, allowing customers to upgrade and reconfigure systems by adding new modules, replacing existing modules, and adding and redeploying systems. Throughout the Cisco Catalyst 6500 Series, modules are:

- *Configurable*—Separately, simplifying the addition of new services
- *Interoperable*—In the same chassis, providing flexible design options
- *Interchangeable*—Among Cisco Catalyst 6500 Series systems, simplifying sparing and network expansion
- *Hot-swappable*—Without requiring a chassis to be powered off, providing fast upgrade and repair
- *Upgradable*—As newer modules come along, providing investment protection

Cisco Catalyst 6500 Series Hardware-Forwarding Architectures

Cisco Catalyst 6500 Series modules use one of three forwarding technologies, each having a different architecture with different characteristics and capabilities:

- *Cisco Express Forwarding (CEF)*—Scaling to 30 Mpps, this technology uses a central CEF Cisco Express Forwarding engine located on the supervisor engine's policy feature card (PFC) daughter and CEF forwarding tables located on the supervisor engine. The supervisor engine makes all forwarding decisions for all interface modules centrally. For more information see *How Cisco Express Forwarding Works.*
- *Accelerated Cisco Express Forwarding (aCEF)*—Suited for high-performance enterprise environments, this technology uses the aCEF engine and aCEF tables located on the interface module, along with the central CEF engine located on the supervisor engine's PFC daughter card and central CEF forwarding tables located on the supervisor engine. The interface module makes high-volume forwarding decisions locally, and the supervisor engine makes the rest of the forwarding decisions centrally. For more information see *How Accelerated Cisco Express Forwarding (aCEF) Works.*
- *Distributed Cisco Express Forwarding (dCEF)* —Suited for the most demanding environments, this technology uses the dCEF engine located on the interface module's distributed forwarding card (DFC) daughter card and the dCEF table, a local copy of the supervisor engine's central CEF table located on the interface module's DFC. The interface module makes all the forwarding decisions locally, and provides maximum performance and scalability. For more information see *How Distributed Cisco Express Forwarding (dCEF) Works*

Cisco Catalyst 6500 Series Switching Architectures

Cisco developed the following switching architectures for Cisco Catalyst 6500 modules to allow platforms to scale in any deployment:

- 32-Gbps bus—Allowing access to a central shared bus
- 256-Gbps switch fabric—Located on the switch fabric module (SFM)
- 720 Gbps switch fabric—Located on Cisco Catalyst 6500 Series Supervisor Engine 720

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0574
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

5.292
A.

Cisco Catalyst 6500 Series Modules

Cisco Catalyst 6500 Series interfacecmodules support the following forwarding technology and switch fabric combinations:

- *Classic Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to the 32-Gbps switching bus only, and forward packets at up to 15 Mpps
- *CEF256 Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to both the 256-Gbps fabric located on the supervisor engine with a single 8-Gbps full-duplex fabric connection and the 32-Gbps switching bus, and forward packets at up to 30 Mpps
- *dCEF256 Interface Modules*—Use the distributed CEF engine on the DFC (located on the interface module), connect to a 256-Gbps fabric located on the supervisor engine or a Switch Fabric Module with 16-Gbps full-duplex fabric connections, and forward packets at up to 210 Mpps
- *aCEF720 Interface Modules*—Use the accelerated CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with 40-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, peak performance
- *dCEF720 Interface Modules*—Use the distributed CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with dual 20-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, sustained performance

Note: All Performance numbers refer to IPv4 forwarding.

Cisco Catalyst 6500 Series Module Types

In the Cisco Catalyst 6500 Series architecture, special-purpose modules perform separate tasks—allowing the feature set to evolve quickly and allowing customers to add new features and enhanced performance by adding new modules. The Cisco Catalyst 6500 Series features the following types of special-purpose modules:

- *Supervisor engines*—Perform the control functions and make the forwarding decisions for packets routed to other networks
- *Ethernet interface modules*—Provide IEEE-standard receive and forwarding interfaces and forward packets within the defined network
- *WAN interface modules*—Provide the receive and forwarding interface at the WAN edge
- *Services modules*—Support multigigabit security, application-aware Layer 4 through 7 content switching, network management, and voice gateway services to traditional phones, fax machines, PBXs, and the PSTN
- *Switch Fabric Modules (SFMs)*—Pass network traffic from interface module to the supervisor engine or to another interface

Cisco Catalyst 6500 Series Supervisor Engines

The supervisor engines for the Cisco Catalyst 6500 Series support different forwarding technologies and achieve different forwarding rates, depending on the configuration of the supervisor engine and the capability of a particular interface module.

Supervisor engines can be configured with optional factory-installed daughter cards—a Policy Feature Card (PFC) providing hardware-based Layer-2 forwarding, and a Multilayer Switch Feature Card (MSFC) providing Layer 3 capabilities.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0575
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.291
A.

A supervisor engine performs control operations centrally on processors that run either Cisco IOS Software or Cisco Catalyst Operating System Software while special-purpose application-specific integrated circuits (ASICs) perform bridging and routing (based on Cisco Express Forwarding), QoS marking and policing, and access control. The same ASICs are used on the DFCs, daughter cards that can be installed on certain interface modules to distribute forwarding in a decentralized fashion to achieve system forwarding rates of up to 400 Mpps (Table 2).

For additional information about the following Cisco Catalyst 6500 Series supervisor engines visit: http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Solution and market	Wiring closet	Enterprise distribution, core, and WAN edge; service provider WAN and Internet edge	Enterprise core and data center; service provider metro; wireless; national research networks; grid computing
Fabric architectures supported	Centralized forwarding only—engine located on supervisor engine's PFCx daughter card	Centralized CEF—engine located on supervisor engine's PFCx daughter card; Distributed CEF—engine located on interface module's DFC daughter card	Centralized CEF—engine located on Supervisor Engine 720's PFC3 daughter card; Distributed CEF—engine located on interface module's DFC3 daughter card; Accelerated CEF—engine located on interface module's ASICs
Fabric connections	32-Gbps shared bus connection to modules	16 Gbps per slot; Dual-fabric connection to modules at 8 Gbps full duplex per channel	40 Gbps per slot; Dual-fabric connection to modules at 20 Gbps full duplex per channel
Performance maximum (Mpps)	15 Mpps	210 Mpps	Sustained 400 Mpps—dCEF720 Peak 400 Mpps—aCEF720
DFC modules	Not supported	DFC	DFC3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0576
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.290
A.

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Route processor	On MSFC2 daughter card (optional)	On MSFC2 daughter card (optional)	MSFC3 integrated
PFC modules	PFC daughter card (optional)	PFC2 integrated	PFC3 integrated

Ethernet Interface Modules

Cisco Catalyst 6500 Series Ethernet interface modules, designed for wiring closet, distribution and core, and data center applications, as well as service provider and Metro Ethernet environments, use one of the following types of Ethernet interfaces:

- *10/100 Mbps over copper and 10/100/1000 Mbps Ethernet over copper*—For wiring closets providing 10/100- and 10/100/1000-Mbps performance with auto-negotiation and inline power for voice; up to 48 ports/module; includes Classic and CEF256 interface modules.
- *100 Mbps over fiber*—For secure wiring closets and long-haul router and switch interconnects; up to 24 ports per module; includes Classic and CEF256 interface modules.
- *1 Gbps*—For distribution and core layers and for data centers providing 1-Gbps performance in a 48-port module; includes Classic CEF256, and dCEF256 interface modules.
- 10 Gbps—For distribution and core layers providing 10-Gbps performance in 1-port or 2-port module; includes CEF256, aCEF720, and dCEF720 interface modules.

For more information, visit:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

WAN Interface Modules

The Cisco Catalyst 6500 Series and Cisco 7600 Series support several WAN interfaces using two technologies:

- *FlexWAN module*—Accepts up to two plug-in port adapters that provide numerous WAN/MAN protocols and features
- *Optical Services Module (OSM)*—A dedicated line card that provides several interfaces, including OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, Channelized T3, Channelized OC-12/STM-4 PoS, Gigabit Ethernet, OC-12/STM-4 ATM, and OC-48/STM-16 Dynamic Packet Transport (DPT)

FlexWAN Module

The FlexWAN module fits inside Cisco Catalyst 6500 Series and Cisco 7600 Series systems and uses Cisco 7200 and 7500 Series port adapters for a wide range of WAN/MAN protocols, including Frame Relay, ATM, PoS, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC). Additionally, the FlexWAN module provides media options such as clear channel and Channelized T1/E1, T3/E3, High-Speed Serial Interface (HSSI), OC-3 PoS, and ATM.

- For information about the Cisco Catalyst 6500 Series and Cisco 7600 Series FlexWAN Module, visit:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a00800923bf.html

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0577
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.289
A.

Optical Services Modules

OSMs are line cards that provide high-speed WAN connectivity with onboard network processors for distributed-line-rate IP service applications. For more information about OSMs, see the following data sheets:

- Cisco 7600 Series 4-, 8-, and 16-Port OC-3c/STM-1 PoS/SDH OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092249.html
- Cisco 7600 Series 4-Port Gigabit Ethernet OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223d.html
- Cisco 7600 Series 1-Port Channelized OC-12/STM-4 to DS3/E3 OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092250.html
- Cisco 7600 Series 1-Port OC-48c/STM-16 PoS/SDH/OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092241.html
- Cisco 7600 Series 2- and 4-Port OC-12c/STM-4 PoS/SDH OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223e.html
- Cisco 7600 Series 2-Port ATM OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008008876f.html
- Cisco 7600 Series 2-Port OC-48c/1-Port OC-48c DPT OSM: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080088774.html

Layer 4 Through 7 Services Modules

The Cisco Catalyst 6500 Series offers an extensive set of services modules for Layer 4 through 7 applications, including content services, network monitoring, security, and telephony.

Content Services Modules

- *Content Services Gateway (CSG)*—Enables differentiated billing, user balance enforcement, and activity tracking for customer billing systems. For more information, visit: http://mobiletraining.cisco.com/csg/CSGe_ds_0211.pdf
- *Content Switching Module (CSM)*—Integrates advanced content switching into the Cisco Catalyst 6500 Series to provide high-performance, high-availability load balancing of caches, firewalls, Web servers, and other network devices. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800887f3.html

Network Monitoring

- *Network Analysis Module (NAM 1 and 2)*—Provides application-level visibility into the network infrastructure for real-time traffic analysis, performance monitoring, and troubleshooting; performs traffic monitoring with embedded Web-based traffic analyzer. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800a2c89.html

Security Services Modules

- *Firewall Services Module (FWSM)*—The FWSM allows any port in the chassis to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet0[illegible]
- *Intrusion Detection System Module (IDSM and IDSM-2)*—Takes traffic from the switch backplane at wire speed, integrating IDS functions directly into the switch. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a0080092341.html

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0578
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.283
CA.

- *IPSec VPN Module (IVSM)*—Provides infrastructure-integrated IPSec VPN services capable of 1.9-Gbps Triple Data Encryption Standard (3DES) performance, 8000 active tunnels, and up to 60 tunnels per second. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe2.html
- *SSL Services Module (SSM)*—Offloads processor-intensive tasks related to securing traffic with SSL accelerating the performance and increasing the security of Web-enabled applications. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800c4fe9.html

Telephony Services Modules

- *Communications Media Module (CMM)*—Provides flexible, high-density T1 and E1 gateways, allowing organizations to connect their existing time-division multiplexing (TDM) networks to their IP communications networks, and providing connectivity to the PSTN. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet09 186a00800e9c1f.html

Switch Fabric Modules

Designed to support distributed forwarding for interface modules that have distributed forwarding capability, the Cisco Catalyst 6500 Series SFM or SFM2, in combination with the Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2 and DFCs on interface modules, increases available system bandwidth from 32 to 256 Gbps. The SFM/SFM2 supports the Cisco Catalyst 6500 CEF256 and dCEF256 interface modules.

Designed to support new interface modules with 720 Gbps forwarding capabilities, the Supervisor Engine 720's onboard switch fabric increases available bandwidth to 720 Gbps and enables packet forwarding rates up to 400 Mpps. By using auto-sensing and auto-negotiation, the Supervisor 720 switch fabric is fully interoperable with the 8- and 16-Gbps switch fabric interconnections used by the CEF256 and dCEF256 interface modules. When a CEF256 or dCEF256 interface module is detected, the switch fabric will automatically connect those modules by offering 8-16 Gbps of bandwidth to each module, as applicable.

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wirespeed, independent of the number of flows transiting the switch.

REQ nº 03/2005 - CN
CPMI - CORREIOS
0379
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.251
A-

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

How Accelerated Cisco Express Forwarding (aCEF) Works

Accelerated Cisco Express Forwarding (aCEF) technology uses two forwarding engines working together in a master-slave relationship to accelerate high-rate traffic flows through the switch—a central CEF engine located on the Supervisor Engine 720's PFC3 and a scaled-down distributed aCEF engine located on the interface module.

The central PFC3 makes the initial forwarding decision, with the aCEF engine storing the result and making subsequent packet-forwarding decisions locally. aCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 is loaded with the necessary CEF information before any user traffic arrives at the switch.
- As traffic arrives on an aCEF720 interface module, the aCEF engine inspects the packet, and finding that no specific packet forwarding information exists, consults the central PFC3.
- The PFC3 makes a hardware-based forwarding decision for this packet (including Layer 2, Layer 3, ACLs, and QoS).
- The aCEF engine stores the forwarding decision results and makes forwarding decisions locally for subsequent packets based on packet-flow history.
- The aCEF engine handles hardware-based Layer 2 and Layer 3 forwarding, ACLs, QoS marking, and NetFlow.
- The central PFC3 processes any forwarding decisions that the interface module's aCEF engine cannot handle.

aCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 and aCEF720 (WS-X67xx) class modules.

How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0580
Doc. 3690

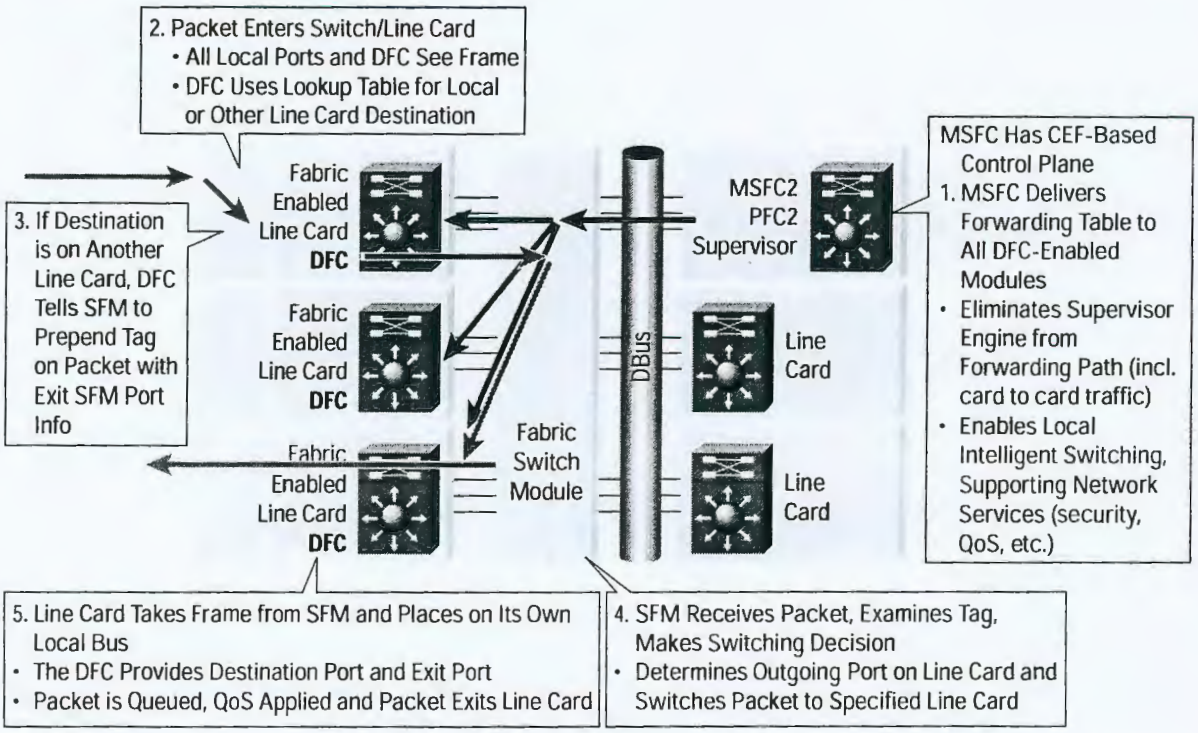
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.286
A.

Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

Figure 6
Distributed Cisco Express Forwarding Packet Flow



dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for the dCEF720 interface module; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2 with PFC2 and a SFM for the dCEF256 interface module.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0581
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-285
A.

Cisco IOS Software and Catalyst Operating System Software

Cisco Catalyst 6500 Series switches offer two operating modes of software, the Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC, and Cisco IOS Software for the supervisor engines. Each operating mode can be deployed at different hierarchies of the network, depending on the network's requirements. These software solutions for the Cisco Catalyst 6500 Series switches provide full Layer 2 through 4 switching and routing functions at high performances.

Today, either of these operating modes can be deployed in an entire network environment, or the operating modes can vary within an environment to meet different requirements. One operating mode is not a replacement for another, but is recommended for varying feature requirements.

- Cisco IOS Software for the Cisco Catalyst 6500 Series
- Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC

Cisco IOS Software for the Cisco Catalyst 6500 Series

Cisco IOS Software for the Cisco Catalyst 6500 Series supervisor engines requires the MSFC on the supervisor engine. It provides integrated multilayer functions in a single image and is optimized for core, distribution, Internet access, and data center deployments. Cisco IOS Software combined with the performance of the Cisco Catalyst 6500 Series offers the necessary features for a high-performance Layer 3-enabled deployment, including support for a distributed architecture with the ability to scale the switch to 400 Mpps throughput. Additionally, Cisco IOS Software provides operational ease of use by offering a single image and configuration file to be deployed across the Cisco Catalyst 6500 Series switches.

Cisco Catalyst Operating System Software with Optional Cisco IOS Software on the MSFC

Cisco Catalyst Operating System Software is the premier software for the wiring closet on Cisco Catalyst 6500 Series switches offering high-performance Layer 2 forwarding. It is optimized to deliver the high availability, enhanced security, and integrated inline power support necessary for mission-critical wiring closet deployments. Cisco Catalyst Operating System Software can also be extended to the distribution and core layers of the network when coupled with Cisco IOS Software on the MSFC, providing robust and advanced Layer 3 and Layer 4 functions. This operating mode is often referred to as "hybrid mode." See Table 3 for software and hardware deployment options.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0582
Fls. Nº
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-284
A.

Table 3 Software and Hardware Deployment Options

Network Performance	Wiring Closet	Distribution/ Data Center	Core	WAN Edge
Highest-performance Cisco IOS Software end-to-end	Cisco IOS Software; Supervisor Engine 2-MSFC2; CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF720 and aCEF720 interface modules
Higher-performance mixed operating system	Cisco Catalyst Operating System Software; Supervisor Engine 2-PFC2; CEF256 and Classic interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and, CEF256 interface modules
High-performance Cisco Catalyst Operating System Software end-to-end	Cisco Catalyst Operating System Software; Supervisor Engine 1-2GE; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; dCEF720 Series and aCEF720 interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules

Cisco IOS Software and Cisco Catalyst Operating System Software Shared Features

All Cisco Catalyst 6500 Series supervisor engines, including the new Supervisor Engine 720, take advantage of the industry-leading software and management capabilities of the Cisco Catalyst 6500 Series. Customers can apply their knowledge of Cisco Catalyst Operating System Software, Cisco IOS Software, CiscoWorks, and other graphical and Web-based network management tools without the need to learn a new command-line interface (CLI) or management system.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0583
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.283
A.

Cisco Catalyst 6500 Series Chassis

Cisco Catalyst 6500 Series chassis can be deployed in the wiring closet, the distribution and core layers, the data center, and the WAN edge, providing the power and features required for end-to-end deployment for the enterprise campus, the ISP network, metro, and research computing networks.

Chassis Applications

The Cisco Catalyst 6500 Series provides a selection of chassis, including 3-, 6-, 9-, and 13-slot models with slots arranged horizontally and a 9-slot model with slots arranged vertically, with front-to-back airflow. Typical applications for Cisco Catalyst 6500 Series chassis include:

- *3-slot chassis*—Low-density, wiring-closet chassis sharing interface modules and supervisor engines with larger chassis for common sparing; low-density, high-performance specialized services modules chassis for network security and management; low-density, high-end chassis providing connectivity to the WAN edge
- *6- and 9-slot chassis*—Traditional chassis for the wiring closet, distribution and core, data center, and WAN edge
- *13-slot chassis*—Highest-capacity chassis for Ethernet connectivity, with slots to spare for services modules providing network security and management

Chassis Configuration

All Cisco Catalyst 6500 Series chassis are NEBS Level-3 compliant and use common power supplies. The 6- and 9-slot chassis require a 1000W or 1300W power supply and the 13-slot chassis requires a 2500W or 4000W power supply. The 3-slot chassis requires a 950W power supply. When ordering a Cisco Catalyst 6500 Series switch, use the online Cisco Dynamic Configuration Tool to assist you in selecting the chassis, power supplies, power cables, and fan trays that will meet your requirements. The tool is available at:
http://www.cisco.com/appcontent/apollo/configureHomeGuest.html

Power

All Cisco Catalyst 6500 chassis hold up to two load-sharing, fault-tolerant, hot-swappable AC or DC power supplies. Only one supply is required to operate a fully loaded chassis. If a second supply is installed, it operates in a load-sharing capacity. The power supplies are hot-swappable—a failed power supply can be removed without powering off the system.

Cisco Catalyst 6500 Series switch power supplies are available in five power ratings:

- 950W AC input (Cisco Catalyst 6503 chassis)
- 1000W AC input
- 1300W AC and DC input
- 2500W AC and DC input
- 4000W AC input

Table 4 outlines the power requirements and heat dissipation for the three different models of power supplies available for the Cisco Catalyst 6500 Series switch.

ECT - 03/2005 - CN
CPMI - CORREIOS
Fls. 0584
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.282
A.

Table 4 Power Supply VAC and VDC requirements

Power Supply	AC Input Voltage/Current	DC Input Voltage/Current
950W	100 to 240 VAC (10% for full range); 15 A	-48 VDC to –60 VDC continuous; 38 A @ –48 VDC, 30 A @ –60 VDC
1000W	100 to 240 VAC (10% for full range); 12 A @ 100 VAC, 6 A @ 240 VAC	Not supported
1300W	100 to 240 VAC (10% for full range); 17.25 A @ 100 VAC, 8 A @ 200 VAC	–48 VDC to –60 VDC continuous; 38 A @ –48 VDC, 30 A @ –60 VDC
2500W	100 to 120 VAC, 200 to 240 VAC (10% for full range); 16 A maximum at 200 VAC at 2500 W output; 16 A maximum at 100 VAC at 1300 W output	–48 VDC to –60 VDC continuous; 80 A @ –40.5 VDC, 70 A @ –48 VDC, 55 A @ –60 VDC
4000W	100 to 240 VAC (10% for full range); 23 A	Not supported

Fan Trays

Chassis that have a Supervisor Engine 720 installed require a high-speed fan tray. See Table 5 for part number information.

Table 5 Catalyst 6500 Chassis Fan Tray Part Numbers

Catalyst 6500 Chassis	Normal Speed Fan— Fan Tray Part Number	High Speed Fan— Fan Tray Part Number
6503	FAN-MOD-3	FAN-MOD-3-HS(=)
6506	WS-C6K-6SLOT-FAN	WS-C6K-6SLOT-FAN2
6509	WS-C6K-6SLOT-FAN	WS-C6K-9SLOT-FAN2
6509-NEB	WS-C6509-NEB-FAN	WS-C6509-NEB-FAN2
6509-NEB-A	N/A	FAN-MOD-09(=)
6513	WS-C6K-13SLOT-FAN	WS-C6K-13SLOT-FAN2

Dimensions

Table 6 provides Catalyst 6500 Series chassis dimensions.

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
H x W x D (in.)	7 x 17.37 x 21.75 in.	20.1 x 17.2 x 18.1 in.	25.2 x 17.2 x 18.1 in.	33.3 x 17.2 x 18.1 in.	18.1 in.
H x W x D (cm)	17.8 x 44.1 x 55.2 cm	51.1 x 43.7 x 46.0 cm	64.0 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm

CPMI - CORREIOS
0385
Fls. Nº 3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-281
A.

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Rack units (RU); 1.75 in., 4.4 cm	4 RU	12 RU	15 RU	20 RU	20 RU

Weight

Table 7 provides the weight information for empty and fully configured Catalyst 6500 Series chassis.

Table 7 Catalyst 6500 Series Chassis Weights

Weight	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Chassis only (lb)	27	45	55	55	98
Fully configured (lb)	83	115	135	135	240
Chassis only (kg)	12	20	25	25	45
Fully configured (kg)	38	52	61	61	109

RQS nº 03/2005 - CN
CPMI - CORREIOS
0586
Fls. Nº
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.280
CA.

Ordering Information

Table 8 provides part number information for Catalyst 6500 Series chassis

Table 8 Catalyst 6500 Series Chassis Part Numbers

Part Number	Chassis
WS-C6503	Cisco Catalyst 6503 chassis (three slots)
WS-C6506	Cisco Catalyst 6506 chassis (six slots)
WS-C6509	Cisco Catalyst 6509 chassis (nine slots)
WS-C6509-NEB	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)
WS-C6509-NEB-A	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)–enhanced
WS-C6513	Cisco Catalyst 6513 chassis (13 slots)

Environmental Conditions

Table 9 provides environmental information for Catalyst 6500 Series Chassis.

Table 9 Catalyst 6500 Series Chassis Environmental Conditions

Parameter	Performance Range
Operating temperature	32 to 104 F (0 to 40 C)
Storage temperature	–4 to 149 F (–20 to 65 C)
Relative humidity	10 to 90%, noncondensing
Operating altitude	3000 meters
Mean time between failure (MTBF)	7 years for system configuration

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0587
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.279
A.

Regulatory Compliance

Safety

- UL 1950
- EN 60950
- CSA-C22.2 no. 950
- IEC 60950
- AS/NZA 3260
- 21 CFR 1040
- EN 60825-1
- IEC 60825-1
- TS 001

EMC

- FCC (CFR 47, Part 15) Class A
- VCCI
- CE Marking
- EN 55022
- EN 55024
- CISPR 22
- AS/NZS 3548
- NEBS Level 3 (GR-1089-CORE, GR-63-CORE)
- ETSI ETS-300386-2

RQS nº 03/2005 - CN
CPMI - CORREIOS
0588
Fls. Nº
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.278
A.

Specifications

Table 10 provides an overview of Catalyst 6500 Series switches specifications, additional information can be found in software release notes.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
IEEE Compliance		
802.1	802.1d	Bridging
	802.1p, q	VLAN tagging
	802.1s	Per-VLAN Group Spanning Tree Protocol
	802.1w	Rapid Spanning Tree Protocol
	802.1x	
802.1	802.3	10BASE-T, 10BASE-FL
	802.3ad	Link aggregation
	802.3ab	1000BASE-T
	802.3ae	10 Gigabit Ethernet
	802.3u	100BASE-TX, 100BASE-FX
	802.3x	Flow control
	802.3z	1000BASE-SX, 1000BASE-LX
RFC Compliance		
ATM	1483, 2584	Protocol encapsulation over ATM AAL-5
		ATM permanent virtual circuit (PVC) to 802.1q tagging
BGP4	1269	Definitions of Managed Objects for the Border Gateway Protocol (Version 3)
	1745	Border Gateway Protocol/Open Shortest Path First (BGP/OSPF) interactions
	1771	BGPv4
	1965	BGP4 autonomous system confederations
	1966	BGP4 route reflection
	1997	Communities attribute
	2385	Transmission Control Protocol (TCP) MD5 authentication for BGP
	2439	Route flap dampening
	2796	Route reflection
	2842	Capabilities advertisement
General routing protocols	768	User Datagram Protocol (UDP)
	783	Trivial File Transfer Protocol (TFTP)
	791	IP

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0589
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	792	Internet Control Message Protocol (ICMP)
	793	TCP
	826	Address Resolution Protocol (ARP)
	854	Telnet
	894	IP over Ethernet
	903	Reverse Address Resolution Protocol (RARP)
	906	TFTP Bootstrap
	951, 1542	BootP, BootP extensions
	1027	Proxy ARP
	1122	Host requirements
	1256	ICMP Router Discovery Protocol (IRDP) IPv4 router discovery
	1519	Classless interdomain routing (CIDR)
	1541	Dynamic Host Control Protocol (DHCP)
	1591	Domain Name System (DNS) client
	1619	PPP over SONET
	1662	PPP HDLC-like framing
	1812	IPv4
	2131	BootP/DHCP
	2338	VRRP
		Internetwork Packet Exchange Routing Information Protocol/ Service Advertising Protocol (IPX RIP/SAP)
		Software-controlled redundant ports
IP multicast	1112	Internet Group Management Protocol (IGMP)
	1122	Host extensions, Distance Vector Multicast Routing Protocol (DVMRP)
	2236	IGMP v1, v2, v3 IGMP v1, v2, v3 Snooping
	2283	Multicast Border Gateway Protocol (MBGP)
	2362	Protocol-Independent Multicast (PIM)-SM
		DVMRP v3-07 Multicast Source Discovery Protocol (MSDP)
		PIM-Dense Mode (PIM-DM) v1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0590
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.276
A.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		PIM-DM v2 Bidirectional PIM (Supervisor Engine 720 only)
Intermediate system to Intermediate system (IS-IS)	1195	TCP
	1377	PPP
	2763	Dynamic host name exchange
	2966	Domain-wide prefixes
LSP tunnels	2211	Controlled load network element service
	2702	Traffic engineering over MPLS
MPLS	2547	MPLS VPN
	2961	Resource Reservation Protocol (RSVP) refresh
	3031	MPLS architecture
	3032	MPLS label stack encoding
	3036	Label Distribution Protocol (LDP)
OSPF	1583	OSPF v2
	1587	OSPF NSSA
	1745	OSPF interactions
	1765	OSPF database overflow
	1850	OSPF v2 Management Information Base (MIB), traps
	1997	Communities and attributes
	2154	OSPF digital signatures, MD5
	2178	OSPF v2 (superceded by RFC 2328)
	2328	OSPF v2
	2370	OSPF opaque link-state advertisement (LSA) option
	2385	TCP M5
	2439	Route flap damping
	2842	Capabilities advertisement
	2918	Route refresh capability
RIP	1058	RIP v1
	1723	RIP v2
	2453	RIP v2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0591
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.275
J.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
Miscellaneous protocols	1866	HTML
	2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
	2068	HTTP
Denial of service (DoS) protection	2267	Network Ingress Filtering
		ACLs: wire-speed
		ICMP and IP-option control
		IP broadcast forwarding control
		Rate limiting using ACLs
		Unicast Reverse Path Forwarding (RPF)
		Server load balancing with Layer 3 and Layer 4 protection
		SYN attack protection
		Session control
Network management	782	VLAN Trunking Protocol (VTP)
	783	TFTP
	854	Telnet
	951	BOOTP
	1155	Structure of Management Information (SMIv1)
	1156	TCP/IP MIB
	1157	Simple Network Management Protocol (SNMP)v1
	1212	MIB definitions
	1213	SNMP MIB II
	1215	SNMP traps
	1256	ICMP router discovery
	1285	Station management (SMT) 7.3
	1354	IP forwarding table MIB
	1493	Bridge MIB
	1516	Ethernet repeater MIB
	1573	Interface table MIB
	1643	Ethernet MIB
	1650	Ether-like MIB

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0592
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	1657	BGPv4 MIB
	1724	RIPv2 MIB
	1757	RMON MIB
	1850	OSPFv2 MIB
	1901, 1907	SNMPv2c
	1908	SNMPv1/v2 coexistence
	2021	RMON2 probes
	2037	ENTITY-MIB
	2096	IP forwarding
	2233	Interface MIB
	2613	RMON analysis for switched networks (SMON) MIB
	2668	802.3 media attachment unit (MAU) MIB
	2787	VRRP MIB
	2925	Ping/Traceroute/NS Lookup MIB
		Sampled Netflow
		999 local messages
		BSD Syslog with multiple servers
		Configuration logging
		CISCO-CDP-MIB
		CISCO-COPS-CLIENT-MIB
		Cisco Discovery Protocol
		CISCO-ENTITY-FRU-CONTROL-MIB
		CISCO-PAGP-MIB
		CISCO-STACK-MIB
		CISCO-STP-Extensions-MIB
		Cisco Traffic Director Software
		CISCO-UDLDP-MIB
		CiscoView
		CISCO-VLAN-Bridge-MIB
		Cisco VLAN Director Software
		CISCO-VLAN-Membership-MIB

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0593
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.273
A.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		CISCO-VTP-MIB
		Cisco Workgroup MIB
		SPAN and Remote SPAN (RSPAN)
		Hot Standby Routing Protocol (HSRP)
		HC-RMON
		HTML/HTTP management
		NetFlow v1 export
		RMON HP Open View
		SMON-MIB
		Standard Cisco IOS Software security capabilities: passwords and TACACS+
		Telnet client
		Telnet management
		Text-based CLI
		Web-based GUI Management Tools (CiscoWorks)
Security	1492	Terminal Access Controller Access Control System Plus (TACACS+)
	2138	Remote Authentication Dial-In User Service (RADIUS) authentication
		ACLs for Layers 2, 3, 4, and 7
		Access profiles on all routing protocols
		Access profiles on all management methods
		Media Access Control (MAC) address security/lockdown
		Network Address Translation (NAT)
		Network login (including DHCP/RADIUS integration)
		RADIUS accounting
		RADIUS per-command authentication
		Secure Copy Protocol (secure file transfer)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0594
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15272
A

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

For additional information about the following data sheets that describe Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0595
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-271
D.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0596
Doc. 3690

Cisco Systems

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

MH/LW4273 0403

15.210
A.

Switch Tipo 1 doc 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0597
Doc. 3690

Cisco Systems

15.269
A.

Data Sheet

Cisco Catalyst 6500 **Supervisor** Engines 1A and 2

As Cisco's premier modular multilayer switch, the Catalyst® 6500 Series delivers secure, converged services from the wiring closet to the core, to the data center to the WAN edge.

The supervisor engines for the Catalyst 6500 Series deliver the latest advanced switching technology with proven Cisco software to power a new generation of scalable and intelligent multilayer switching solutions for both enterprise and service provider environments. Designed to integrate data, voice, and video into a single platform for fully integrated IP communications, the Catalyst 6500 Series supervisor engines enable intelligent, resilient, scalable, and secure high performance multilayer switching solutions.

The widely deployed Supervisor Engine 1A and Supervisor Engine 2 are used in wiring closets, distribution/core, data center and WAN edge configurations enabling the seamless integration of advanced services such as security, voice and content into a converged network that reduces the total cost of ownership. And the new Supervisor Engine 720 is ideally suited for high performance core, data center and metro Ethernet deployments with its scalable performance of up to 400 million packets per second using a 720Gbps switch fabric.

By sharing a common set of interfaces, operating system and management tools, the Catalyst 6500 Series supervisors provide operational consistency—enabling common sparing and minimizing training requirements; all modules feature predictable performance and a broad range of capabilities. Supervisor Engine 1A and Supervisor Engine 2 highlights include:

- *Feature-rich and wire-rate intelligent network services*—Support and complement comprehensive security and granular Quality of Service mechanisms, including identity-based networking capabilities based on IEEE 802.1x extensions and simplified configuration using two AutoQoS commands
- *End-to-end flexible deployments*—Position anywhere in the network from the wiring closet to the distribution/core, and from the data center to the WAN edge and the MAN
- *Scaleable and predictable performance*—Feature a flexible switch fabric and forwarding architecture delivering throughput from 15Mpps/32Gbps (Classic interface modules), to 30Mpps/256Gbps (CEF256 interface modules), to 210Mpps/256Gbps (dCEF256 interface modules) for network cores supporting multi-gigabit trunks
- *Flexible multilayer switching support and forwarding architectures*—Select basic Layer 2 forwarding or feature-rich Cisco Express Forwarding (CEF) using the same supervisor

ECT/ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0508
3690
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

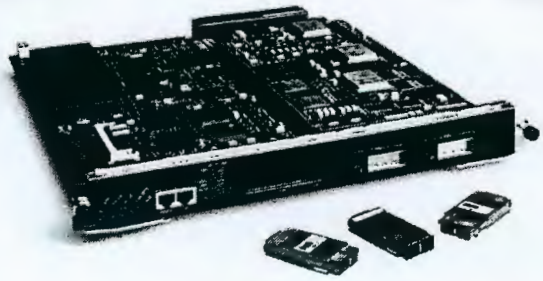
15-268
A

- *Choice of operating system support*—Support both Cisco IOS® Software, Catalyst OS software, and Hybrid (Catalyst OS software and Cisco IOS Software for the MSFC)
- *Operational consistency*— Support all 3 generations of Catalyst 6500 Series interface and services modules in all Catalyst 6500 3-, 6-, 9- and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software and a common set of Cisco network management tools that support the Catalyst 6500 Supervisor Engine 1A and 2 as well as many other Cisco Systems product lines
- *Maximum network uptime and user productivity*—Provide fault-tolerant network resilience and high availability features including fast 1- to 3-second stateful fail-over between redundant Catalyst 6500 supervisor engines enabling near-hitless software upgrades for business critical network environments, including IP-telephony enabled wiring closets
- *Extensive management tools*—Support CiscoWorks network management platform, Simple Network Management Protocol (SNMP) versions 1, 2, and 3 and four RMON groups (statistics, history, alarms, and events)

As part of the Catalyst 6500 Series of modular products, Supervisor Engines 1A and 2 share a common operating system and CLI—encouraging an end-to-end Catalyst 6500 Series solution for maximum operational consistency, common sparing, and minimized training requirements (Figure 1).

Figure 1 Supervisor Engines 1A and Supervisor Engine 2

Supervisor Engine 1-PFC



Supervisor Engine 2-MSFC2

RQS nº 03/2005 - CN
CPMI - CORREIOS
0599
Fls. Nº
3690
Doc.

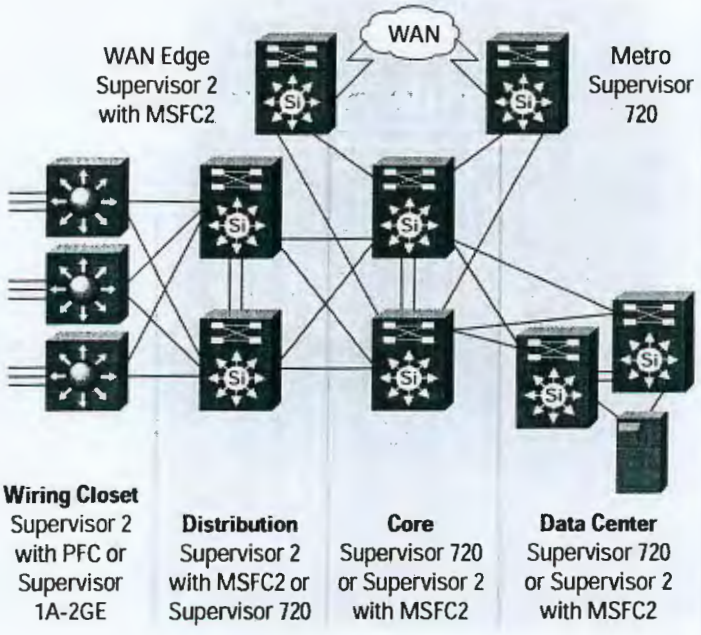
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.267
JA

Supervisor Engine 1A and Supervisor Engine 2 Deployment Scenarios

With a broad range of interfaces, and services modules, chassis / slot configurations as well as a scalable set of Supervisor Engines, the Catalyst 6500 can be deployed anywhere in the network. The figure below depicts the Catalyst 6500 deployed in the wiring closet, distribution, core, data center, WAN edge and Metro and provides recommended supervisor engines for each part of the network.

Figure 2
Cisco Supervisor Engine 1A and Supervisor Engine 2 Deployment Scenarios



RQS nº 03/2005 - CN
CPMI - CORREIOS
0600
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.266
A.

The following table outlines the primary deployment scenarios for Cisco Catalyst 6500 Series supervisor engines.

Table 1 Deployment Scenarios for Cisco Catalyst 6500 Series Supervisor Engines

Supervisor Engine	Performance/Features	Recommended Deployments
Supervisor Engine 720	400 Mpps, 720 Gbps Layer 2–4 distributed Cisco Express Forwarding Supports new accelerated Cisco Express Forwarding 720 and distributed Cisco Express Forwarding 720 interface modules	Enterprise core, distribution, and data centers
Supervisor Engine 2 **Policy Feature Card 2 (PFC2)** **Multilayer Switch Feature Card 2 (MSFC2)**	210 Mpps, 256 Gbps Layer 2–4 distributed Cisco Express Forwarding Supports distributed Cisco Express Forwarding 256 interface modules	Enterprise distribution, data centers, and WAN edge
Supervisor Engine 1A **PFC** **MSFC2**	15 Mpps, 32 Gbps Centralized Layer 2–4 forwarding Enhanced security and quality of service (QoS)	Distribution and core
Supervisor Engine 2 **PFC2**	30 Mpps, 256 Gbps Centralized Layer 2 forwarding and Layer 3–4 services Enhanced security and QoS	Premium wiring closet and data center access
Supervisor Engine 1A **PFC**	15 Mpps, 32Gbps Centralized Layer 2 forwarding and Layer 3–4 services Enhanced security and QoS	Enterprise wiring closets
Supervisor Engine 1A **2GE**	15 Mpps, 32 Gbps Centralized Layer 2 forwarding	Value wiring closet

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0601
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.265
A.

Supervisor Engine 1A and 2 Features

The Supervisor Engine 1A and 2 provide the following features:

- High availability
- Scalable performance
- Wire-rate traffic management
- End-to-end management tools
- Comprehensive security
- Advanced Layer 2, Layer 3, and Layer 4 forwarding

High Availability

Supervisor Engines 1A and 2 can be deployed in dual-supervisor engine configurations in all Cisco Catalyst 6500 Series chassis (6503, 6506, 6509, and 6513). The dual-supervisor engine configuration synchronizes protocol states between the primary and the redundant supervisor engine, provides industry-leading network availability with sub-3-second failover, and maximizes network uptime by allowing hot swapping of standby supervisor engines. Important high-availability features include:

- *Supervisor engine redundancy*—With synchronization of protocol states and support for HSRP and Uplink Fast
- *Rapid failover rates*—Sub-3-second stateful failover and Layer 3 IP Unicast and Multicast failover
- *Hot swapping*—Hot swapping of standby supervisors

Scalable Performance

Supervisor Engines 1A and 2 provide scalable performance, from 15 Mpps to 210 Mpps with bandwidth scaling from 32 Gbps to 256 Gbps, that densely populated wiring closets and high-throughput network cores with multigigabit trunks require.

Supervisor Engine 2 uses the Cisco Express Forwarding routing architecture that performs high-speed lookups even with advanced Layer 3 services enabled, and independent of the number of flows through the switch, while maintaining 30 Mpps of centralized performance and 210 Mpps of distributed performance.

- *Supervisor Engine 1A*—Provides 15-Mpps performance with 32-Gbps bandwidth
- *Supervisor Engine 2*—Provides 30 Mpps of centralized performance and 210 Mpps of distributed performance with 256-Gbps bandwidth

For details see Table 2—Cisco Catalyst 6500 Supervisor Engine Feature Comparison.

Wire-Rate Traffic Management

Supervisor Engines 1A and 2 provide wire-rate traffic management using Layer 2, 3, and 4 QoS and security checks, including ACL policy enforcement, as part of their forwarding process to protect and secure content. These traffic management features enable efficient handling of converged networks that carry a mix of mission-critical, time-sensitive, and bandwidth-intensive multimedia applications.

- Advanced QoS tools such as packet classification and marking and congestion avoidance based on Layer 2, Layer 3, and Layer 4 header information.
- QoS scheduling rules with thresholds can be configured in the switch for multiple receive and transmit queues.
- Rate limiting can be used to police traffic on a per-flow or aggregate basis with a very fine granularity.

For details see Table 3—QoS Features Comparison.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0602
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.264
A-

End-to-End Management Tools

Managed with CiscoWorks2000, Cisco Catalyst 6500 Series switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Cisco Resource Manager, a Web-based management tool that works with CiscoWorks2000, provides: automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Supervisor Engines 1A and 2 provide a comprehensive set of management tools to provide the required visibility and control in the network.

- *Console management*—Provide shared interface to the Supervisor Engine 2 and the Multilayer Switch Feature Card 2 (MSFC2) available out-of-band from a local terminal or remote terminal connected through a modem to the console or auxiliary interface
- *In-band management*—Provide shared interface to the Supervisor Engine 2 and the MSFC2 available in-band through SNMP, Telnet client, Bootstrap Protocol (BOOTP), and Trivial File Transfer Protocol (TFTP)
- *SPAN*—Allow management and monitoring of switch traffic
- *RSPAN*—Allow centralized management and monitoring by aggregating and directing traffic from multiple distributed hosts and switches to a remotely located switch through a trunk link
- *VACL Capture*—Direct traffic to a network analysis port using an ACL

For details see Table 4—Management Tools Comparison.

Comprehensive Security

The advanced security capabilities of Supervisor Engines 1A and 2 can reduce the threats of malicious attacks while enabling authentication, authorization, and accounting. With support for up to 32K ACL entries, IP/IPX security ACLs in hardware, and advanced features such as port security, Supervisor Engines 1A and 2 offer a superior set of Layer 2–4 network traffic security capabilities:

- *Layer 2 security features*—Include private VLANs and port security, to help the network architect properly partition and control the utilization of the switch resources.
- *Layer 2, 3, and 4 hardware filters*—Can work on the forwarding engine and in conjunction with optional integrated services modules to inspect each forwarded packet and permit or deny all the streams of traffic according to the network administrator's rules.

For details see Table 5—PFC and PFC2 Security Features Comparison.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0603
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.263
A-

Supervisor Engine 1A and 2 Architecture

Catalyst 6500 Series Supervisor Engines 1A and 2 manage the system by storing and running the system software, controlling the various modules in the chassis, performing basic forwarding, and providing the Gigabit uplinks that allow redundant supervisor engine connections.

Supervisor Engine 2 offers an improved forwarding design. The Supervisor Engine 1A CPU performs Layer 2 forwarding, but Supervisor Engine 2 performs Cisco Express Forwarding (CEF) and distributed CEF, doubling the forwarding performance. As shown in Table 2, Supervisor Engines 1A and 2 offer choices in operating characteristics, including forwarding architecture, performance, bandwidth, DRAM and boot Flash sizes, and support for chassis, Policy Feature Card/Policy Feature Card 2 (PFC/PFC2), MSFC2, and Switch Fabric Module (SFM).

Table 2 Cisco Catalyst 6500 Supervisor Engine Feature Comparison

Feature	Supervisor Engine 2 *Supervisor Engine-PFC2* *Supervisor Engine-MSFC2*	Supervisor Engine 1A *Supervisor Engine 1A-2GE* *Supervisor Engine 1A-PFC* *Supervisor Engine 1A-/MSF*
Cisco Express Forwarding (CEF)	Yes	No
Performance	30 Mpps—*Supervisor Engine 2- PFC2 and Supervisor Engine 2-MSFC2* up to 210 Mpps—*Supervisor Engine 2- MSFC2 with SFM and DFCs*	15 Mpps
Maximum bandwidth	256 Gbps (with distributed forwarding)	32 Gbps
DRAM	128 MB, 256 MB, 512 MB	128 MB
Onboard Flash (BootFlash)	32 MB	16 MB
Chassis supported	6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, 6513; 7603, 7606, 7609, OSR-7609, 7613	6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A; 7603, 7606, 7609, OSR-7609
PFC daughter card available	Yes (PFC2); Standard with Supervisor Engine 2	Yes (PFC); Not field upgradable
MSFC2 daughter card available	Yes, and field upgradable	Yes, not field upgradable
SFM supported	Yes	No

The PFC/PFC2 and MSFC2 daughter cards and the SFM increase Supervisor Engines 1A and 2 functions:

- *PFC and PFC2*—Perform hardware-based Layer 2, Layer 3, and Layer 4 packet forwarding as well as packet classification, traffic management, and policy enforcement
- *MSFC2*—Performs Layer 3 control plane functions including address resolution and routing protocols
- *SFM 2*—Provides 256 Gbps dedicated bandwidth to all slots in the chassis and requires Supervisor Engine 2-MSFC2. The SFM 2 will not operate in the same chassis with Supervisor Engine 720.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0604
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.261
A.

Policy Feature Card (PFC and PFC2)

The Policy Feature Card provides quality of service (QoS) and policy based intelligent networking capabilities to the Catalyst 6500 Series. Recommended for premier wiring closets, backbone, data center and WAN edge deployments, the PFC identifies and classifies traffic applying the appropriate QoS priority level and Security Policies as defined by the network administrator configured ACLs. The PFC also helps to prevent unauthorized applications from being allowed on the network.

The Supervisor Engine PFC daughter card makes the packet forwarding decision in its application-specific integrated circuit (ASIC) complex. In distributed forwarding implementations, an identical ASIC complex located on an interface module's DFC daughter card allows the interface module to make packet-forwarding decisions locally. After the PFC or DFC makes the forwarding decision for the interface module, it sends the forwarding result to the interface module that does all packet buffering, queuing, and delivery.

In addition to packet forwarding, the PFC performs the following major functions at wire-rate:

- *Layer 3 packet classification*—Using QoS access-control entries
- *Traffic management (rate limiting)*—Using ingress and egress policing
- *Security policy enforcement*—Within subnets or VLANs
- *Intelligent multicast forwarding*—Efficient replication of multicast streams, supplied to appropriate end-user stations
- *NetFlow data export*—Collecting IP flow statistics for inter-subnet flows

QoS

The following table shows the PFC and PFC2 QoS features.

Table 3 QoS Features Comparison

Feature	PFC2 *Supervisor Engine 2* *PFC2* *Supervisor Engine 2* *MSFC2*	PFC *Supervisor Engine* *1A PFC* *Supervisor Engine* *1A PFC/MSFC2*	No PFC *Supervisor Engine* *1A-2GE*
Layer 2 classification and marking	Yes	Yes	Yes
Layer 3 classification and marking/ Access Control Entries (ACEs)	Yes 32K	Yes 16K	None
Rate limiting location (port)	Ingress port, VLAN	Ingress port, VLAN	None
Rate Limiting Level Types ***CIR = Committed Information Rate*** ***PIR = Peak Information Rate***	CIR, PIR	CIR	None
Aggregate traffic rate limiting/ number of policers	Yes 1023 policers	Yes 1023 policers	None
Flow-based rate limiting method/ number of rates	Full flow; 64 rates	Full flow; 64 rates	None

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0605
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.260
A

Management Tools

The following table compares the management tools that are available with Supervisor Engines 1A and 2.

Table 4 Management Tools Comparison

Feature	PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2* *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	No PFC *Supervisor Engine 1A-2GE*
SPAN	Yes	Yes
RSPAN	Yes	No
ERSPAN	No	No
VACL Capture	Yes	No

Security

Table 5 shows the PFC and PFC2 security features.

Table 5 PFC and PFC2 Security Features Comparison

Feature	With PFC2 *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	With PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2*	Without PFC *Supervisor Engine 1A-2GE*
Port security	Yes	Yes	Yes
TCP intercept hardware acceleration	Yes	Yes	No
IEEE 802.1X and 802.1X extensions	Yes	Yes	No
IP security ACLs in hardware	Yes	Yes	No
IPX security ACLs in hardware	Yes	Yes	No
Security ACL entries	32K	16K	No
Reflexive ACLs	128K	512K	No
Unicast Reverse Path Forwarding (uRPF) check-in hardware	Yes	No	No
CPU rate limiters	1	None	None

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0606
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.259
A-

Multi-layer Switch Fabric Card2 (MSFC2)

Supported on both Supervisor 1A and Supervisor 2 as an option the MSFC2 acts as the Layer 3 forwarding routing engine. On its Layer 3 forwarding routing engine, the MSFC2 builds the CEF Forwarding Information Base (FIB) table in software and then downloads this table to the ASICs on the PFC or DFC that make the forwarding decisions for IP Unicast and Multicast traffic. For more information see How Cisco Express Forwarding Works.

Layer 3 Switching

Table 6 shows the MSFC2 Layer 3 switching features.

Table 6 Layer 3 Switching Feature Comparisons

Feature	MSFC2 *Supervisor Engine 1A-PFC/MSFC2* *Supervisor Engine 2-MSFC2*	No MSFC2 *Supervisor Engine 2-PFC2*	No MSFC2 *Supervisor Engine 1A-2GE* *Supervisor Engine 1A-PFC*
IPv4 routing	Yes	Yes, with MSFC2 upgrade	No, not upgradable
MPLS	Yes, through OSM	Yes, through OSM	No
IPv6	Yes, in software (only on Supervisor Engine 2-MSFC2	No, requires MSFC2 upgrade	No

Note: Refer to the release notes for up-to-date software version information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0607
Doc. 3690

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.256
A.

Switch Fabric Modules (SFM and SFM2)

Designed to support distributed forwarding, the Cisco Catalyst 6500 Series SFM (WS-X6500-SFM) and SFM2 (WS-X6500-SFM2) provide dedicated bandwidth to each slot up to 256 Gbps per system.

For distributed forwarding to work, an interface module must have a Distributed Forwarding Card (DFC) and must be installed in the chassis with either a Supervisor Engine 2-MSFC2 and an SFM or SFM2, or a Supervisor Engine 720. The SFM works with Cisco Catalyst 6506, 6509, 6509-NEB, and 6509-NEB-A chassis and can occupy any slot. The SFM2 works with 6506, 6509, 6509-NEB, 6509-NEB-A, 6513, 7603, 7606, 7609, OSR-7609, and 7613 chassis; and it can occupy any slot, except in the 6513 and 7613 where it must occupy slot 7 or 8.

The Catalyst 6503 does not currently support the SFM modules as this would leave one slot open after configuring the supervisor and SFM in two of the three available slots. However, the Supervisor 720 provides full CEF256, dCEF256, aCEF720 and dCEF720 capabilities to the Catalyst 6503 chassis with its slot-efficient integration of the supervisor engine and switch fabric in a single module.

Switch Fabric Module Architecture

Providing access to the switch fabric through dual 8-Gbps serial channels, the SFM or SFM2 performs all switching on the module independent of the passive backplane. For more information see How Distributed Cisco Express Forwarding (dCEF) Works.

High Availability

Two SFM and SFM2 modules can be configured in a system for high availability with 1-to-1 redundancy, where one SFM or SFM2 is operational and one serves as a backup.

Note: The SFM and SFM2 cannot operate in the same chassis with a Supervisor Engine 720.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0608
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.257
A.

Supervisor Engine 2-MSFC2

Suited for deployment in the distribution/core with Classic interface modules, CEF256 interface modules and dCEF256 interface modules, Supervisor 1A-2GE provides Layer 2/3/4 forwarding with the following operational advantages:

- *Layer 2–4 forwarding*—Performs Layer 2 – 4 forwarding with Layer2, 3, 4 features; supports dCEF256 interface modules
- *Media Access Control (MAC) addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—IPv4 supported (See Table 6 for details)
- Distributed forwarding—Requires Switch Fabric Module and interface modules with Distributed Forwarding Cards (DFCs); for details, see section titled How Distributed Cisco Express Forwarding (dCEF) Works
- *Operating system*—Cisco Catalyst OS with Cisco IOS on the MSFC and Cisco IOS Software
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128, 256, 512 MB
- *Onboard flash (BootFlash)*—32 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, and 6513; 7603, 7606, 7609, OSR-7609, and 7613
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None required

Figure 3
Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2

RQS nº 03/2005 - CN
CPMI - CORREIOS
0609
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.256
CA-

Supervisor Engine 2-PFC2

Suited for deployment in wiring closets with Classic and CEF256 interface modules, Supervisor Engine 1A-2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer2, 3, 4 features; requires MSFC2 upgrade to support Layer 3, 4 forwarding
- *MAC addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—Requires MSFC2 upgrade (See Table 6 for details)
- *Distributed forwarding*—Requires MSFC2 upgrade, SFM, and interface modules with DFCs (for details, see section titled How Distributed Cisco Express Forwarding (dCEF) Works).
- *Operating system*—Cisco Catalyst OS only (Cisco IOS Software supported with MSFC2 upgrade)
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128, 256, 512 MB
- *Onboard flash (BootFlash)*—32 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, and 6513; 7603, 7606, 7609, OSR-7609, and 7613
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—MSFC2 upgrade

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0610
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

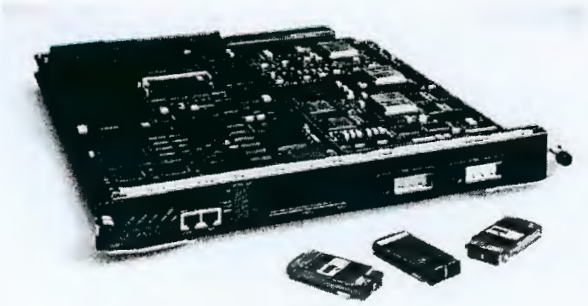
15.255
A-

Supervisor Engine 1A-PFC/MSFC2

Suited for deployment in the distribution/core with Classic interface modules, Supervisor Engine 1A-2GE provides Layer 2–4 forwarding with the following operational advantages:

- *Layer 2–4 forwarding*—Performs Layer 2–4 forwarding with Layer 2–4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (see Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—IPv4 supported (See Table 6 for details)
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS with Cisco IOS on the MSFC and Cisco IOS Software
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None

Figure 4
Cisco Catalyst 6500 Supervisor Engine 1A-PFC/MSFC2



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0611
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

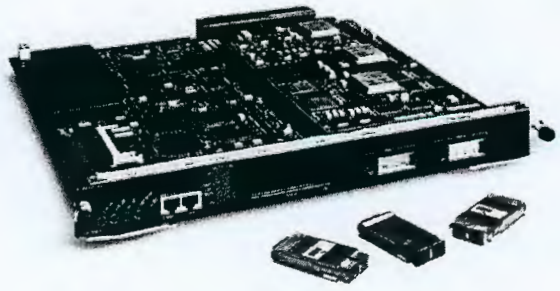
15.254
A-

Supervisor Engine 1A-PFC

Suited for deployment in wiring closets with Classic interface modules, Supervisor Engine 1A–2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs basic Layer 2 forwarding with no Layer 2–4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—Unsupported
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS only
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrades*—None

Figure 5
Cisco Catalyst 6500 Supervisor Engine 1A-PFC



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0612
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.253
A.

Supervisor Engine 1A-2GE

Suited for deployment in wiring closets with Classic interface modules, Supervisor Engine 1A–2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer 4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 only, not upgradable to support Layer 3 (for details, see Table 3—QoS Features Comparison)
- *Multilayer (Layer 3) switching*—Unsupported
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS only
- *Management tools*—SPAN only
- *DRAM*—64 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0613
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.252
A.

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wire-rate, independent of the number of flows transiting the switch.

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

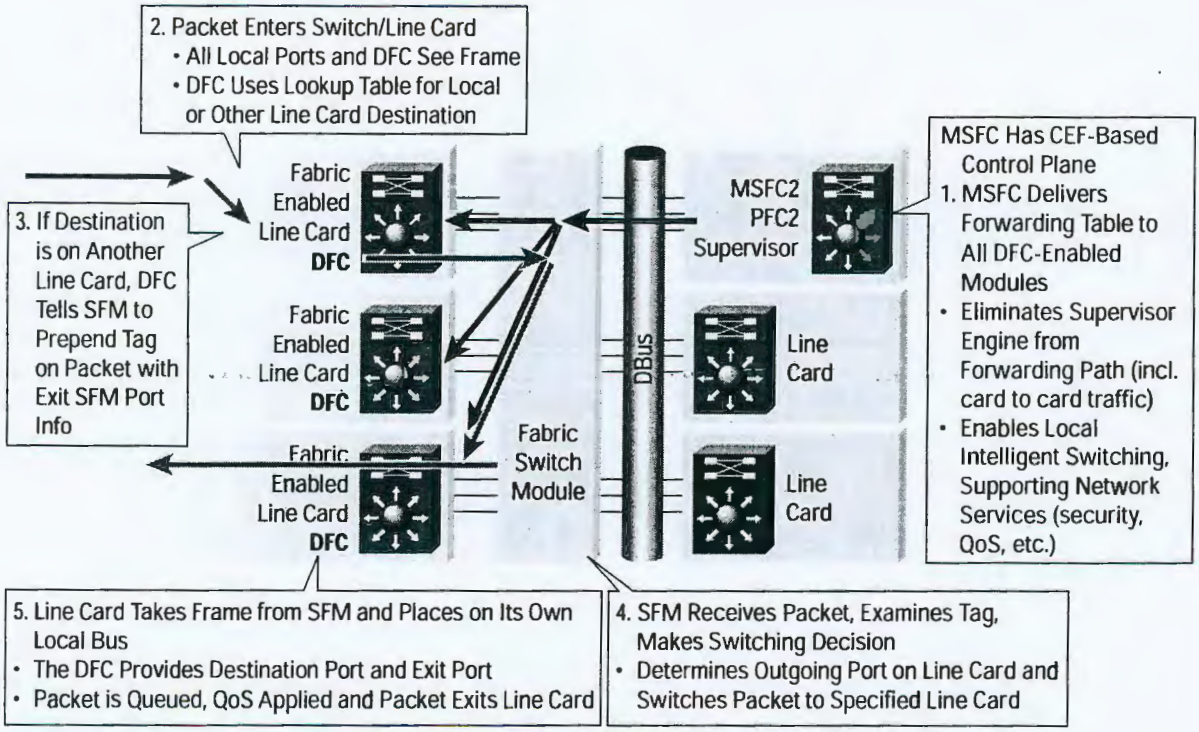
Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0614
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 5
Distributed Cisco Express Forwarding Packet Flow



dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for dCEF720 interface modules; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2-MSFC2 and a SFM for dCEF256 interface modules.

Software Requirements

Depending on its configuration, a supervisor engine will operate with one or more of the following operating systems:

- Cisco IOS Software for the supervisor engine (native Cisco IOS Software)
- Cisco Catalyst OS software
- Hybrid, Catalyst OS software and Cisco IOS Software for the MSFC

Notes: Refer to the release notes for up-to-date software version information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0615
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.230
A.

Ordering Information

Table 7 lists the ordering information for the Supervisor Engines 1A and 2.

Table 7 Product Numbers for Ordering

Product Number	Description
WS-X6K-SUP1A-2GE	Catalyst 6500 Supervisor Engine1A, 2GE
WS-X6K-SUP1A-PFC	Catalyst 6500 Supervisor Engine1A, 2GE, plus PFC
WS-X6K-S1A-MSFC2	Catalyst 6500 Supervisor Engine1A, 2GE, plus MSFC-2 and PFC
WS-X6K-S2-PFC2	Catalyst 6500 Supervisor Engine 2, 2GE, plus PFC-2
WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine 2, 2GE, plus MSFC-2/PFC-2
WS-X6K-S1A-MSFC2	Supervisor Engine 1A with PFC+MSFC2
WS-X6K-S1A-MSFC2=	Supervisor Engine 1A with PFC+MSFC2=
WS-X6K-S1A-MSFC2/2	Supervisor Engine 1A with PFC+MSFC2/2
WS-F6K-MSFC2	Catalyst 6500 Multilayer Switch Feature Card 2
MEM-MSFC2-128MB=	Catalyst 6500 MSFC2 Memory, 128 MB DRAM Spare
MEM-MSFC2-256MB	Catalyst 6500 MSFC2 Memory, 256 MB DRAM Option
MEM-MSFC2-256MB=	Catalyst 6500 MSFC2 Memory, 256 MB DRAM Spare
MEM-MSFC2-512MB	Catalyst 6500 MSFC2 Memory, 512 MB DRAM Option
MEM-MSFC2-512MB=	Catalyst 6500 MSFC2 Memory, 512 MB DRAM Spare
WS-X6500-SFM	Catalyst 6500 Switch Fabric Module
WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module2

Dimensions

- (H x W x D): 1.6 x 15.3 x 16.3 in. (4.0 x 37.9 x 40.3 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Regulatory compliance

RQS nº 03/2005 - CN
CPMI - CORREIOS
0616
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.249
A.

Safety Certifications

- UL 1950
- EN 60950
- CSA-0C22.2 No. 950
- IEC 950

Electromagnetic Emissions Certifications

- FCC 15J Class A
- VCCI CE II
- CE mark
- EN 55022 Class B
- CISPR 22 Class B

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco Systems is committed to maximizing the return on your network investment. Cisco offers a portfolio of Technical Support Services to ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

Cisco Technical Support Services offers the following features, which help enable network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your operations technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement
- The Cisco portfolio of Technical Support Services includes:
- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information visit:

http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0617
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.2.03
A.

Additional Cisco Catalyst 6500 Series Information

For additional information about the Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Catalyst 6500 Series Data Sheet
- Catalyst 6500 Supervisor Engine 720 Data Sheet
- Catalyst 10/100 and 10/100/1000 Ethernet Data Sheet
- Catalyst 6500 Gigabit Ethernet Interface Modules Data Sheet
- Catalyst 6500 10 Gigabit Ethernet Interface Modules Data Sheet
- Catalyst 6500 FlexWAN Interface Modules Data Sheet
- Catalyst 6500 Switch Fabric Interface Modules Data Sheet
- Catalyst 6500 Content Services Module (CSM) Data Sheet
- Catalyst 6500 Firewall Services Module Data Sheet
- Catalyst 6500 Network Application Module (NAM) Data Sheet
- Catalyst 6500 Intrusion Detection (IDS) Module Data Sheet
- Catalyst 6500 IP Sec/VPN Services Module Data Sheet
- Catalyst 6500 SSL Services Module Data Sheet

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

ECT/ECP 08/2005 ON
CPMI - CORREIOS
Fls. N0618
3690
Doc.
203070/ETMG-07/03

15.247
A.

Switch Tipo 1 doc 3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0619
3690
Doc.

Cisco Systems

15.246
A.

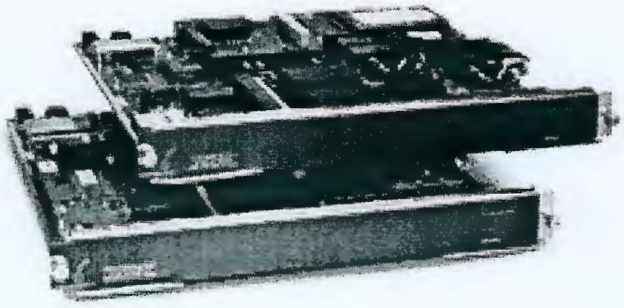
Data Sheet

Cisco Catalyst 6500 Series and Cisco 7600 Series
Network Analysis Module 1 and 2

Second-Generation, High-Performance Network Analysis Modules for Cisco Catalyst 6500 Series and Cisco 7600 Series

Cisco Systems®, the worldwide leader in networking for the Internet, addresses the need for multiservice network management and traffic monitoring in high-capacity switched Ethernet LANs and routed WANs with a new generation of the Network Analysis Module (NAM) for Cisco® Catalyst® 6500 Series switches and Cisco 7600 Series routers. The NAM is an integrated and powerful traffic monitoring service module that occupies a single slot in the chassis and enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing returns on network investments.

The second-generation NAMs are available in two hardware versions, NAM-1 and NAM-2, and offer high performance monitoring and crossbar (fabric) connectivity to meet diverse network analysis needs in scalable switching and routing environments running at gigabit speeds. The NAMs come with an embedded, Web-based traffic analyzer, which provides full-scale remote monitoring and troubleshooting capabilities that are accessible through a Web browser.



Application-Level Visibility Built into the Network

The NAMs give network managers visibility into all layers of network traffic by providing application-level Remote Monitoring (RMON) functions based on RMON2 and other advanced Management Information Bases (MIBs). The NAMs add to the built-in Remote Monitoring (mini-RMON) features in Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that provide port-level traffic statistics at the Media Access Control (MAC) or data link layer. The NAMs provide intelligence to analyze traffic flows for applications, hosts, conversations, and network-based services such as quality of service (QoS) and voice over IP (VoIP).

Integrated Monitoring for LANs and WANs

The NAMS use several data sources from local and remote switches and routers to provide combined visibility into LAN and WAN environments. The NAMs collect data from physical ports, virtual LANs (VLANs), or Cisco EtherChannel®

ECT nº 03/2005 - CN
CPMI - CORREIOS
0620
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

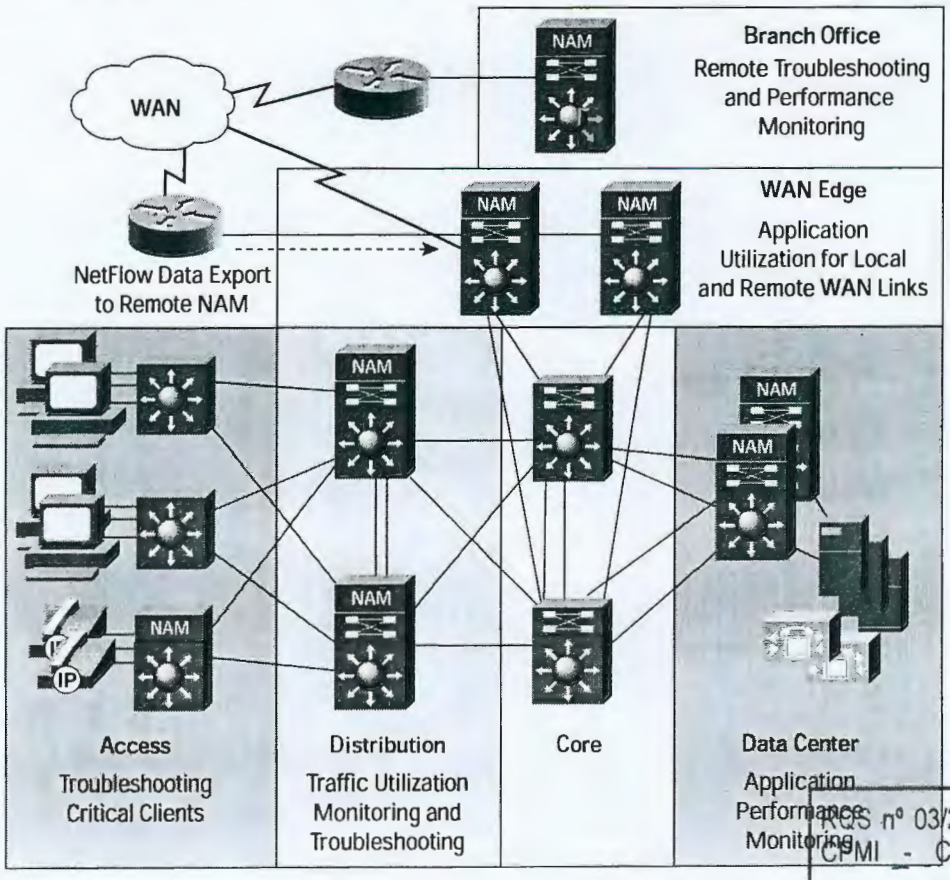
15.245
A.

connections using the Switch Port Analyzer (SPAN) feature. For selective monitoring of large amount of traffic or for traffic from WAN interfaces, VLAN access control list (VACL)-based captures can be used to filter traffic before it is sent to NAM. In addition, the NAMs collect and analyze NetFlow Data Export from local and remote devices to provide broad application-level visibility into the network, including remote WAN segments. The NAMs also collect data from remote switches using the remote SPAN (RSPAN) feature of the Cisco Catalyst switches.

Flexible Deployment Scenarios

The NAMs can be deployed in the Cisco Catalyst 6500 Series at LAN aggregation points (for example, in the core or distribution layer) for proactive monitoring; at service points (for example, in data centers, server farms, or Cisco CallManager clusters in IP telephony networks) where performance is critical; and at important access points (critical clients, IP phone closets) where quick troubleshooting is required. They can also be deployed in Cisco 7600 Series routers at WAN edges or in Catalyst 6500 Series switches connected to WAN routers. When deployed at remote branch offices, the NAMs provide unique advantage to perform remote troubleshooting and traffic analysis through its Web-based Traffic Analyzer without having to send personnel or to haul large amounts of data to the central site. Figure 1 highlights the deployment of NAMs to enable comprehensive traffic monitoring and analysis for performance monitoring, troubleshooting, and capacity planning.

Figure 1
Deploying NAMs to Build Intelligence into the Network to serve a Variety of Applications



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0621
3690
Doc.

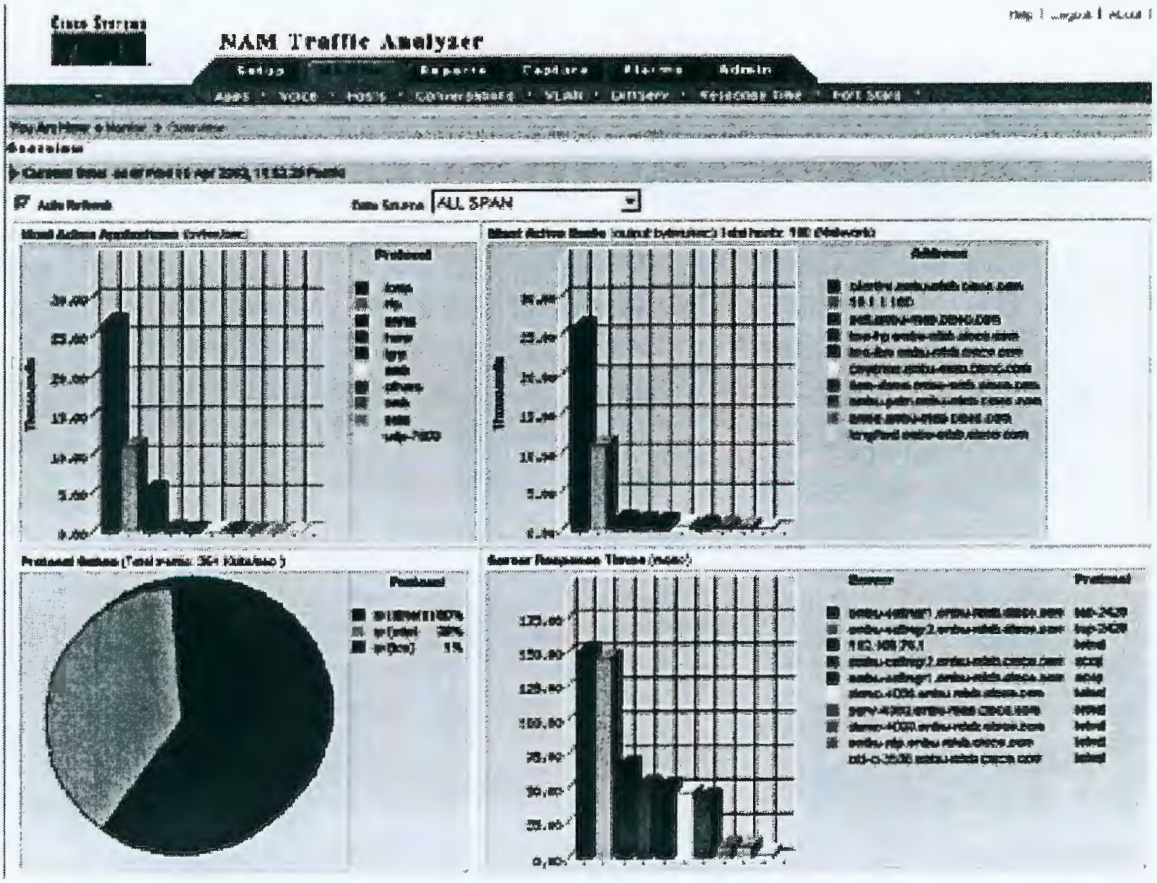
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.244
A.

Easy to Deploy and Use

The NAMs come with the embedded, Web-based Traffic Analyzer with extensive monitoring and troubleshooting capabilities. Because the NAMs integrate monitoring functions directly into the switch and have complete data collection and data analysis capabilities on board, they are easy to deploy and managers can conveniently access data from anywhere using a Web browser (Figure 2). For security, users can be given role-based access and the Web-browser access can be secured with up to 168-bit encryption.

Figure 2
Web-Based Traffic Monitoring for both LAN and WAN with the embedded NAM Traffic Analyzer



The NAMs also provide the flexibility to use standards-based external applications using the Simple Network Management Protocol (SNMP). NetScout *n*Genius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS), collects data from NAMs across the network and provides reports on traffic flow.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0622
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.243
A

Major Benefits

- Increase return on network investment—The visibility provided by the NAMs enables better utilization of network resources to meet business objectives. They ease deployment of network-based services and help in capacity planning.
- Reduce productivity loss and revenue loss—Through proactive monitoring and quick troubleshooting capabilities, the NAMs prevent loss due to network degradation and downtime.
- Enhance network security—The NAMs provide investigation and verification capabilities to supplement other security mechanisms such as intrusion detection and firewalls. They can also be used to detect threats by watching anomalies in the network traffic.

Features and Applications

The data collected by the NAMs can be used for several vital management activities, including real-time and historical application monitoring, performance management, fault isolation, troubleshooting, and capacity planning. The NAMs also play an active role in managing differentiated services such as voice.

Real-Time and Historical Application Monitoring

Using RMON, RMON2, several extended RMON MIBs, and NetFlow, the NAMs detect the applications on the network and provide detailed real-time and historical information about how these applications utilize the bandwidth, which hosts access those applications, and which client/server pairs generate the most traffic (Figure 3A and 3B).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0623
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.242
A.

Figure 3A
Monitoring Applications and Hosts on the Network

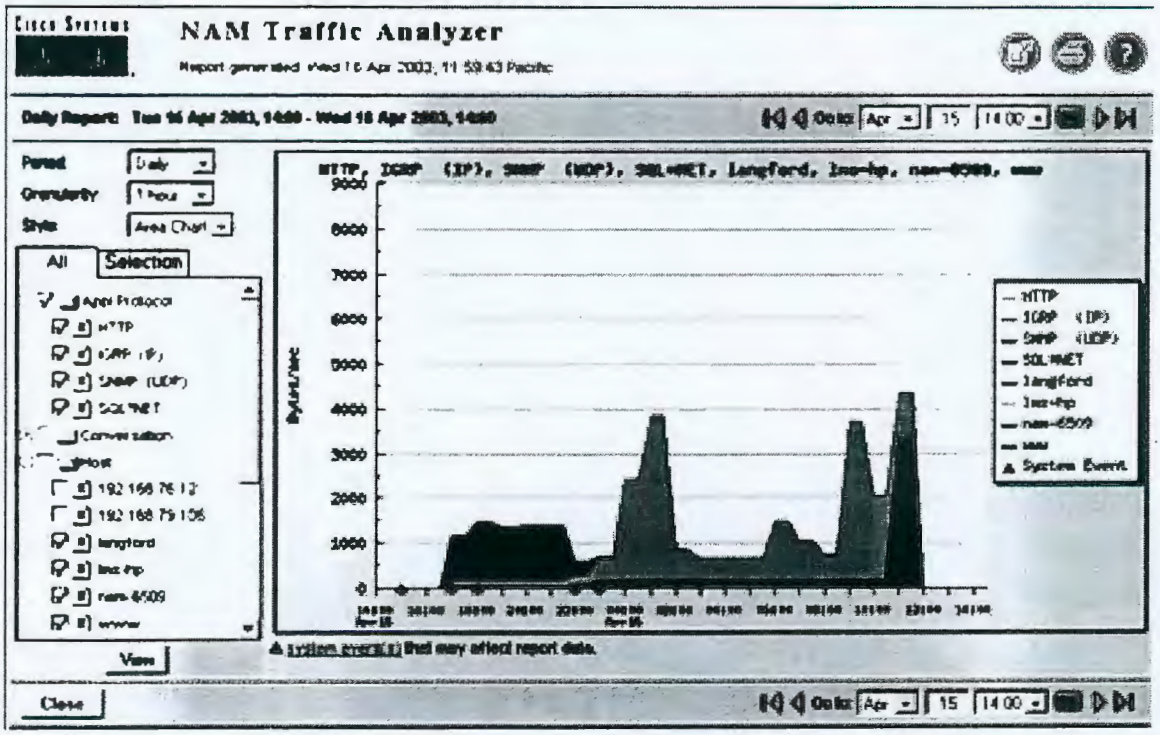
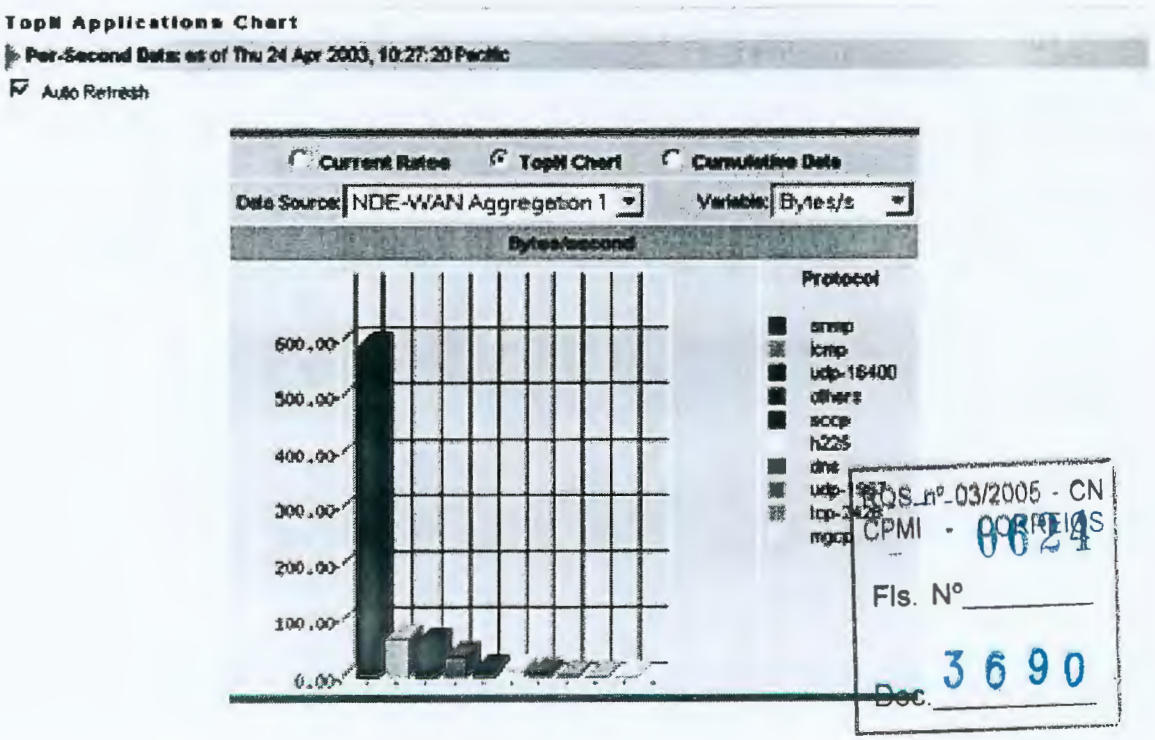


Figure 3B
Monitoring Application Utilization on a WAN link using NetFlow Data Export from a Remote Router



ROS nº 03/2005 - CN
CPMI - CORREIOS
0024
Fls. Nº
3690
Doc.

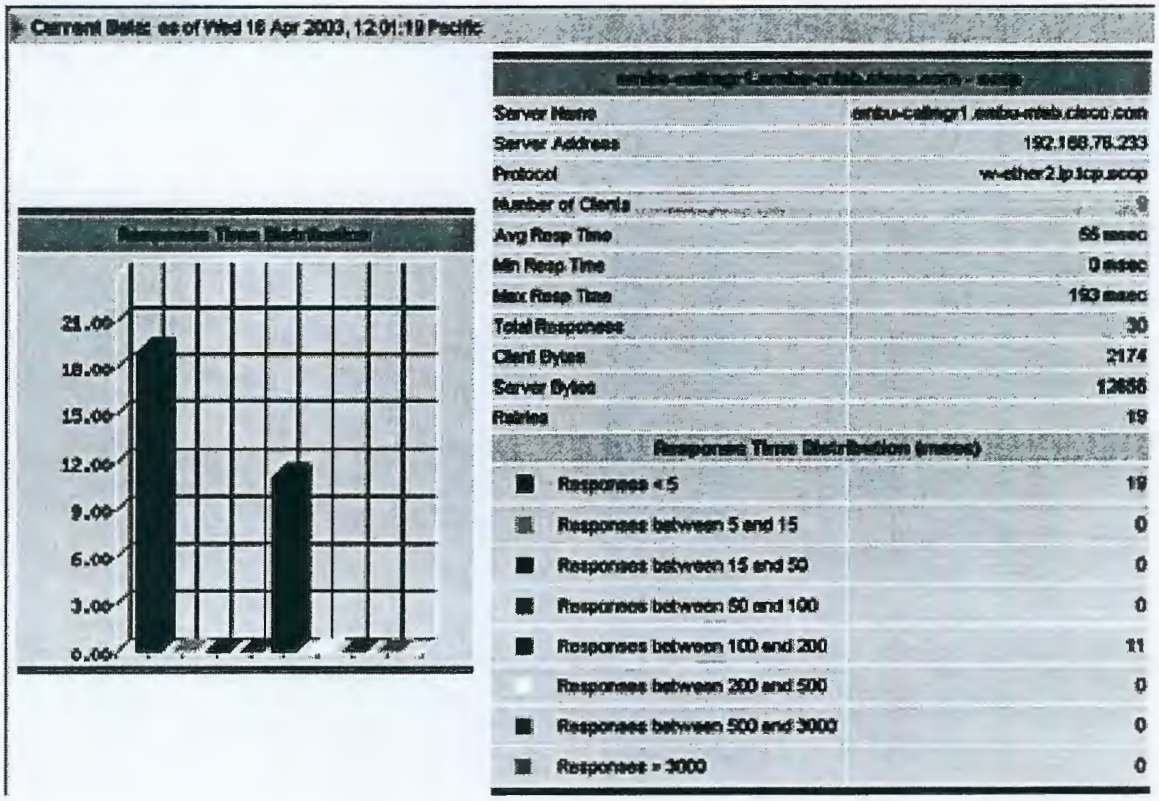
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.241
A.

Performance Management

The NAMs provide valuable information about the delays in server responses to client requests. Using the Application Response Time (ART) MIB, developed by Cisco partner NetScout Systems, the NAMs can identify problems with applications or servers in critical environments such as e-commerce and IP telephony (Figure 4).

Figure 4
Application Response Time Monitoring



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0625
3690
Doc.

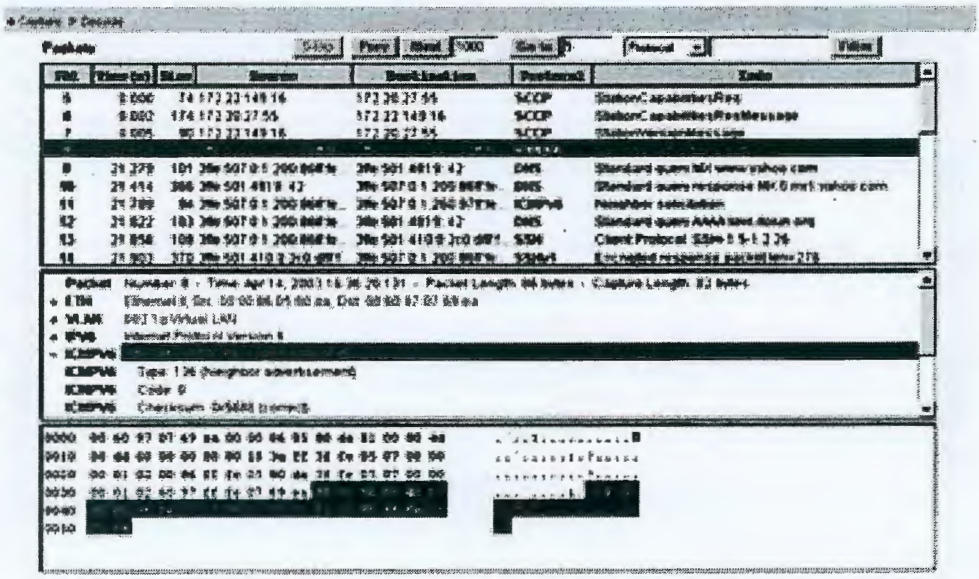
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.240
A.

Fault Isolation and Troubleshooting

Using the NAMs, network managers can set thresholds and alarms on various network parameters such as increased utilization, severe application response delays, and voice quality degradation, and be alerted to potential problems. The NAMs provide comprehensive views on applications, hosts, voice, quality of service (QoS), and so on, to isolate faults or malfunctions in the network. The NAM Traffic Analyzer can capture and decode packets in real time to aid troubleshooting (Figure 5).

Figure 5
Capturing and Decoding Packets with NAM



VoIP and QoS Monitoring

The NAMs can analyze voice traffic flows in real time to collect valuable information, including call setup details and voice quality metrics. Network managers can be alerted to voice quality degradation and can isolate potential problems (Figure 6).

The NAMs make the deployment of QoS for voice and other critical services effective by identifying violations of QoS policies. The NAMs support the Differentiated Services Monitoring (DSMON) MIB, which monitors traffic by differentiated services code point (DSCP) allocations defined by QoS policies (Figure 7).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0626
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.239
A.

Figure 6
IP Telephony Monitoring

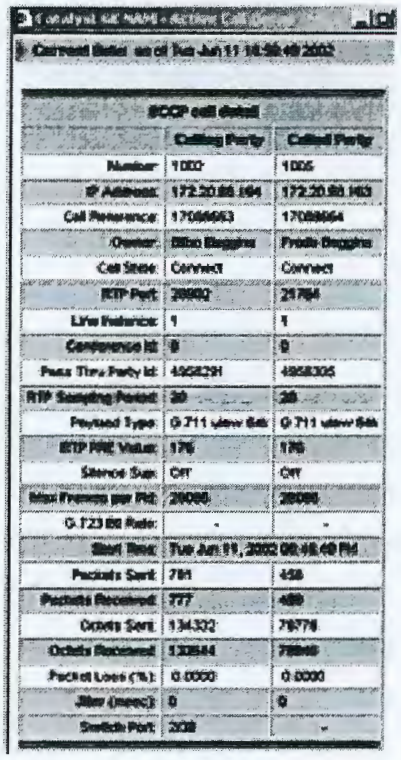
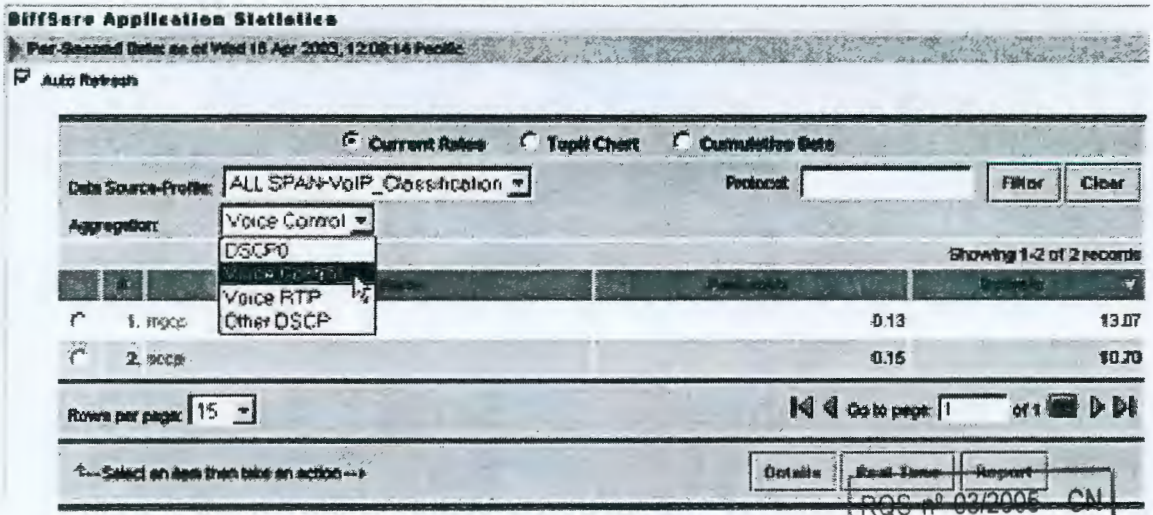


Figure 7
QoS Monitoring Using DSMON



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0627
Doc. 3690

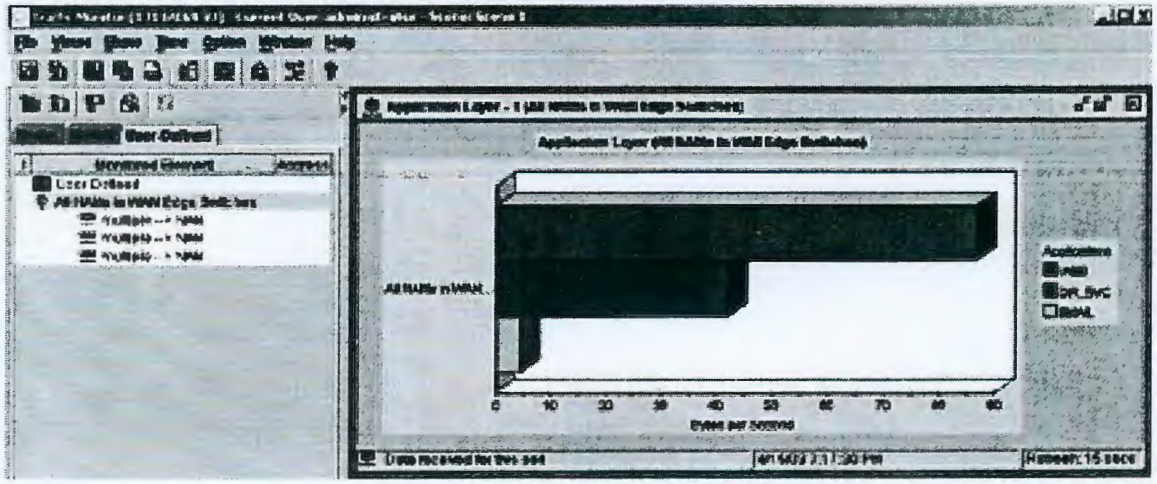
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.233
A.

Capacity Planning and Other Extended Applications

The data from the NAMs across the network can be collected by NetScout nGenius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS) to provide consolidated views of network traffic (Figure 8). The NAMs serve as data sources for several other standards-based applications for a variety of purposes including capacity planning, long-term historical reporting and trending, anomaly-based threat detection, etc.

Figure 8
Aggregating data from NAMs across the network using NetScout nGenius Real-Time Monitor



Primary Advantages

- Integrated with network infrastructure—The NAMs occupy a single slot within the Cisco Catalyst 6500 Series or Cisco 7600 Series chassis and are deployed, managed, and supported as an integral part of the network infrastructure. They do not interfere with switching and routing functions and have their own processing resources. They are managed as a part of the network device using CiscoWorks management tools.
- Complete monitoring solution for LAN, WAN, and network-based services—The NAMs combine the functions of data collection agent and analysis application in one and provide comprehensive monitoring using a variety of data sources including RMON, RMON2 and NetFlow though the embedded Traffic Analyzer.
- Total cost of ownership savings—The integrated nature of the NAM solution saves costs in acquiring network device-specific features like mini-RMON, and in maintenance and technical support. The NAM Traffic Analyzer is embedded in the NAMs at no extra cost.
- Extensible, standards-based solution—The NAMs are compliant with open standards, and can be used with different monitoring applications to meet diverse needs.
- Secure solution—The NAM Traffic Analyzer can be deployed with up to 168-bit encryption, and SNMP can be disabled for fortifying external access to the NAM. The NAMs support Secure Shell (SSH) for secured command-line access.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0628
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.237
A.

Network Monitoring Solutions

Cisco Systems offers a wide variety of solutions to provide complete visibility into network infrastructure. The comprehensive Cisco solution includes embedded technologies such as mini-RMON, NetFlow, Service Assurance Agent (SAA), Network-Based Application Recognition (NBAR); NAMs for the Cisco Catalyst 6500 Series and Cisco 7600 Series for value-added traffic analysis. and CiscoWorks network monitoring applications. nGenius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS), collects mini-RMON data from switches to provide port utilization statistics and uses data from NAMs across the network to provide broad-based analysis and reports on network traffic. Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners extend the Cisco network monitoring solution through a variety of applications that use embedded data sources and NAMs.

Technical Specifications

NAM-1

- High-performance dual processor architecture, 512 MB RAM
- Two data collection interfaces to backplane: 1 for SPAN/VACL data sources, 1 for NetFlow
- Second generation fabric enabled platform with interface to both bus and crossbar based architectures

NAM-2

- Extra high-performance dual processor architecture with hardware-based packet acceleration, 1 GB RAM
- Gigabit monitoring performance
- Three data collection interfaces to backplane: 2 for SPAN/VACL data sources (can be used independently or together), 1 for NetFlow
- Second generation fabric enabled platform with interface to both bus and crossbar based architectures

Supported Platforms

- NAM-1 and NAM-2 can be deployed in any slot in Cisco Catalyst 6500 and 6000 Series switches and Cisco 7600 Series routers [both bus- and crossbar (fabric)-based architectures]; multiple NAMs can be placed in the same chassis
- Supported with Cisco IOS® Software or Cisco Catalyst Operating System on the Supervisor Engine

Supported Topologies and Data Sources

- LAN—Switch Port Analyzer (SPAN) or Remote SPAN (RSPAN), VLAN ACL(VACL)-based captures, NetFlow (v1, v5, v6, v7, v8)
- WAN—NetFlow (v1, v5, v6, v7, v8) from local and remote devices, VLAN ACL (VACL)-based captures for FlexWAN/Optical Service Module (OSM) interfaces (Cisco IOS Software only)

Supported Interfaces and Applications

- HTTP/HTTPS with embedded web based NAM Traffic Analyzer
- SNMP v1, v2 with NetScout nGenius Real Time Monitor and other standards based applications

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0629
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.236
A.

NAM Traffic Analyzer

- Embedded in NAM Software Version 2.2 and later for NAM-1/NAM-2
- Web based—Requires Microsoft Internet Explorer 5.0 or Netscape 4.7 (minimum)
- Supports Secure Sockets Layer (SSL) security with up to 168-bit encryption
- Role-based user authorization and authentication locally or using TACACS+
- Real-time and historical statistics (up to 100 days) on LAN/WAN traffic and network-based services

NAM Software Version 3.1

- Supports NAM-1 (part number WS-SVC-NAM-1), NAM-2 (WS-SVC-NAM-2) and first-generation NAM (WS-X6380-NAM)
- Supported with Cisco IOS® Software Release 12.1(13)E or Cisco Catalyst Operating System 7.3(1) minimum on the Supervisor Engine

Supported MIB Groups

The NAMs are standards-compliant and support RMON and RMON2 MIBs, as well as several extensions. The major MIB groups supported in the NAMs are:

- MIB-II (RFC 1213)—All groups except Exterior Gateway Protocol (EGP) and transmission
- RMON (RFC 2819)—All groups
- RMON2 (RFC2021)—All groups
- SMON (RFC2613)—DataSourceCaps and smonStats
- DSMON (RFC 3287)
- HC-RMON (RFC 3273)
- Application Response Time (ART)

Supported Protocols

The NAMs provide RMON2 statistics on several-hundred unique protocols, including those defined in RFC 2896, and several Cisco proprietary protocols. In addition, the NAMs can automatically detect unknown protocols and users have the flexibility to customize the protocol directory.

Examples of Protocols Supported by the NAMs for RMON2 Statistics:

- TCP and UDP over IP including IPv6
- VoIP including SCCP(Skinny), RTP/RTCP, MGCP, SIP
- Mobile IP protocols (Both IP in IP and GRE tunnelling)
- Storage area network (SAN) protocols including Fiber Channel over TCP/IP
- AppleTalk, DECnet, Novell, Microsoft
- Database protocols including Oracle, Sybase
- Bridge and router protocols
- Cisco proprietary protocols
- Unknown protocols by TCP/UDP ports, RPC program numbers, etc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0630
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

95-235
A.

Physical Specifications

- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm); Occupies any 1 slot in the chassis

Operating Environment

- Operating temperature: 32 F (0 C) to 104 F (40 C)
- Nonoperating and storage temperature: -40 F (-40 C) to 158 F (70 C)
- Operating relative humidity: 10% to 90% (noncondensing)
- Nonoperating relative humidity: 5% to 95% (noncondensing)
- Operating and nonoperating altitude: Sea level to 10,000 ft (3050 m)

Agency Approvals

- Regulatory: CE Marking (89/366/EEC and 73/23/EEC)
- Safety: UL 1950, CAN/CSA-C22.2 No. 950, EN 60950, IEC 60950
- Electromagnetic Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55024, EN50082-1

Ordering Information

Cisco Part Number	Description
WS-SVC-NAM-1	Network Analysis Module-1 for Cisco Catalyst 6500 Series and Cisco 7600 Series
WS-SVC-NAM-2	Network Analysis Module-2 for Cisco Catalyst 6500 Series and Cisco 7600 Series
SC-SVC-NAM-3.1	Network Analysis Module Software v 3.1 for NAM-1, NAM-2 (includes ART, VoIP)

- The use of mini-RMON in Cisco Catalyst 6500 Series and Cisco 7600 Series with NAMs installed does not require the purchase of a separate RMON agent license.
- The Application Response Time (ART) MIB and the VoIP monitoring features are included at no extra cost for the NAM-1 and NAM-2. They require purchase of separate licenses (SC6K-NAM-ART-LIC= and SC6K-NAM-VOIP-LIC=) with the first-generation NAM (WS-X6380-NAM)
- Service Part Numbers for NAM-1 and NAM-2 are CON-xxx-WSSVCNAM1 and CON-xxx-WSSVNAM2 respectively, where "xxx" stands for level of support (for example, xxx= SNT = 8x5x Next Business Day)

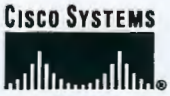
More Information

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0631
3690
Doc.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.234
A-



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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and EtherChannel are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

205059/ETMG_04/03

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3690
Doc.

15.233
A.

Switch Tipo 1 doc 4

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0633
Doc. 3690

Cisco Systems

White Paper

15.232
A.

Catalyst 6000 and 6500 Series **Architecture**

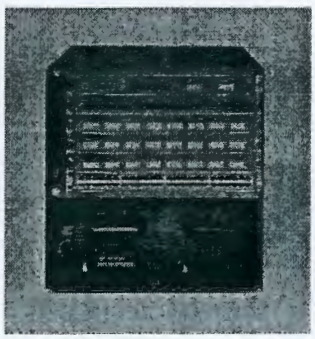
Executive Summary

The ever-increasing demands for bandwidth and performance, and even greater need for intelligent network services, challenge today's switches, routers, and associated devices. Customers require a wide range of performance and services, including high availability, quality of service (QoS), and security, to build scalable enterprise and service provider networks.

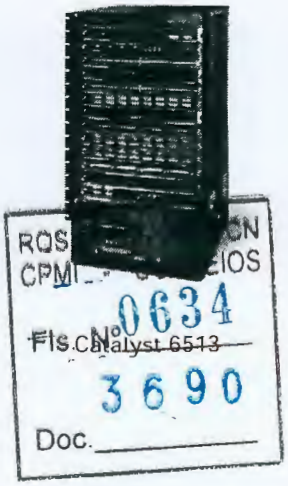
The Cisco Catalyst® 6000 Family, which includes the Catalyst 6000 and 6500 Series, delivers new high-performance, feature-rich, multilayer-switching solutions for enterprise and service provider networks. Designed to address the increased requirements for gigabit scalability, high availability, and multilayer switching in campus backbone and distribution points, Internet data centers, and Web hosting and e-commerce environments, the Catalyst 6000 Family complements the Catalyst 4000 and 3500 families for user aggregation, and the Cisco 7200, 7500, 7600, and Cisco 12000 Gigabit Switch Router (GSR), for high-end routing. Together, the Catalyst and Cisco router families deliver a wide range of intelligent solutions.

The Catalyst 6500 Series architecture supports scalable switching bandwidth up to 256 Gbps and scalable multilayer switching that exceeds 200 million packets per second (pps). For customers not requiring the performance of the Catalyst 6500 Series, the Catalyst 6000 Series provides a more cost-effective solution, with backplane bandwidth of 32 Gbps and multilayer switching that scales up to 15 million pps. The Catalyst 6000 Series architecture provides a superior schema for congestion management by using per-port buffering. In addition, the advanced switching engines of the Catalyst 6500 Series ensure that services such as QoS, security, and policing can be done with no performance degradation.

Catalyst 6509



Catalyst 6506



All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.231
A.

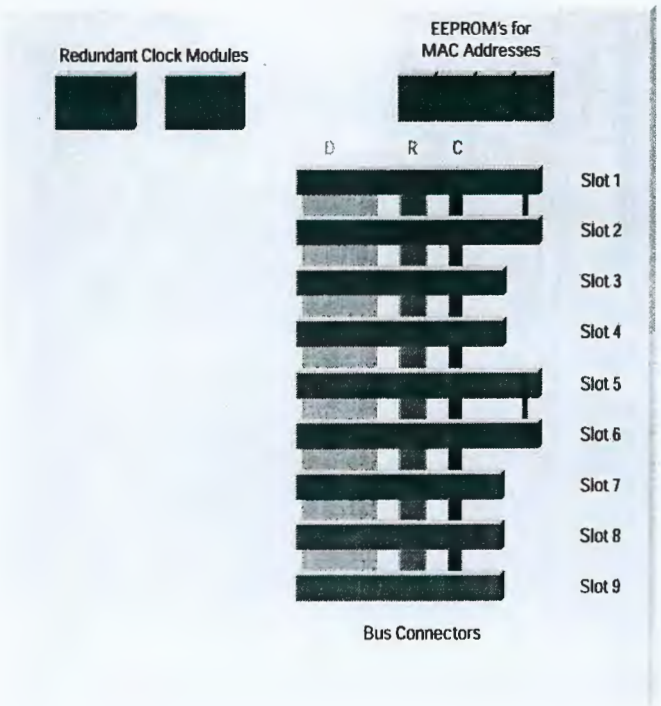
Catalyst 6000 Family Hardware Options

The Catalyst 6000 Family comprises the Catalyst 6000 and 6500 Series Switches. Cisco Systems offers the Catalyst 6000 Family in several different chassis options. Because customers look for modularity in offered slots, the Catalyst 6000 and 6500 offer six- and nine-slot chassis versions. The Catalyst 6500 also offers a 13-slot chassis and a "NEBS" chassis, in which slots are vertically arranged. Both Catalyst 6000 and 6500 Series Switches also support a wide range of interface types and densities, including 384 10/100 Ethernet ports, 192 100Base-FX Fast Ethernet ports, and up to 130 Gigabit Ethernet ports (in the nine-slot chassis). The 13-slot chassis offers up to 576 10/100 ports or 192 Gigabit Ethernet ports.

Backplane layout in the Catalyst 6000 and the Catalyst 6500 differs. The Catalyst 6000 uses a 32-Gbps switching bus. The Catalyst 6500 offers both the 32-Gbps switching bus and the option for the 256-Gbps Switch Fabric Module (SFM). The SFM uses slot 5 (and optionally slot 6 for redundancy) and provides the system with a high-speed switching path. The SFM cannot be used in the Catalyst 6000 Series. The following figures show the backplane layout of the Catalyst 6000 and 6500 Series.

Catalyst Backplanes

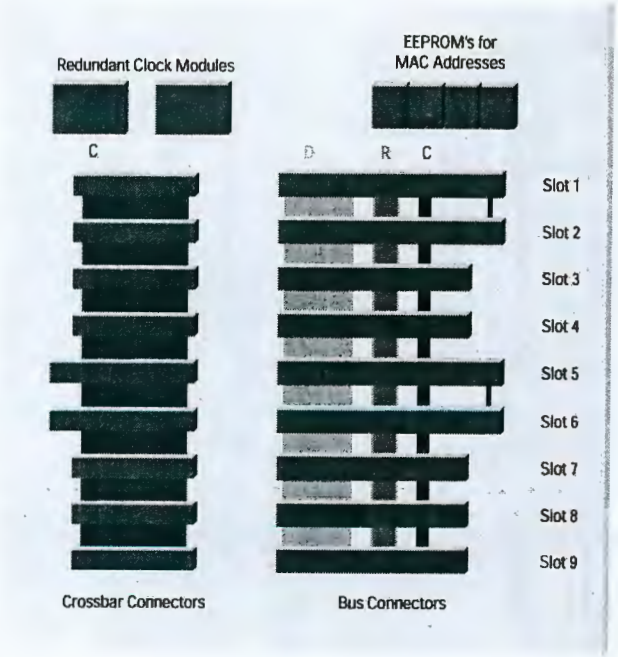
Figure 1 Catalyst 6009 Backplane



RQS nº 03/2005 - CN
CPMI — CORREIOS
0635
Fls. Nº
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 2 Catalyst 6509 Backplane

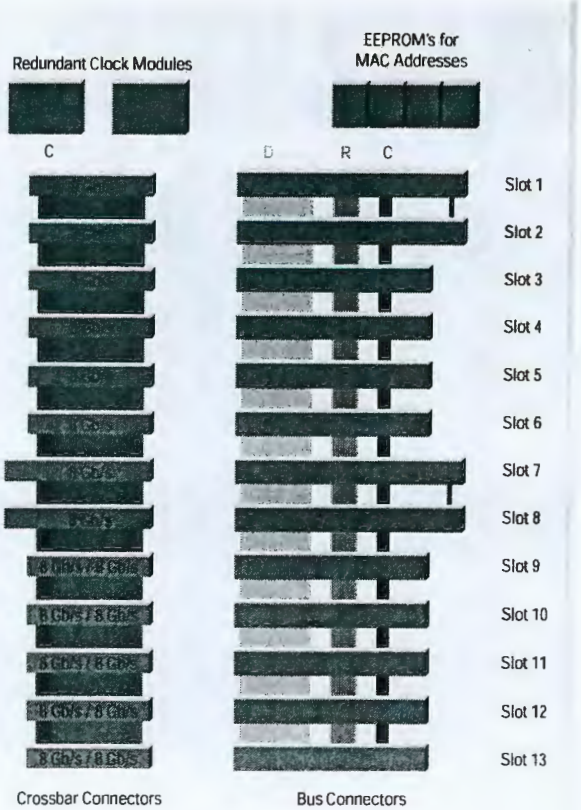


Catalyst 6500

Slot 1—Supervisor Engine
Slot 2—Line Card or Redundant Supervisor Engine
Connectors on Right for:
- EARL Data Bus (Dbus)
- EARL Results Bus (Rbus)
- Ethernet Out of Band Channel (EOBC)

Redundant Clock Modules
MAC Address EEPROMs
Slot 5—Switch Fabric Module
Slot 6—Line Card or Redundant Switch Fabric Module
Connectors on Left for 256 Gbps Crossbar Switching Fabric

Figure 3 Catalyst 6513 Backplane



Catalyst 6513

Slot 1—Supervisor Engine
Slot 2—Line Card or Redundant Supervisor Engine
Connectors on Right for:
- EARL Data Bus (Dbus)
- EARL Results Bus (Rbus)
- Ethernet Out of Band Channel (EOBC)

Redundant Clock Modules
MAC Address EEPROMs
Slot 7/8—Optional Switch Fabric Module Support or Line Card
Supports 2500W/4000W Power Supply
Connectors on Left for 256 Gbps Crossbar Switching Fabric
Slots 2–8 Support 1 * 8 Gb/s Fabric Channel, Slots 9–13 Support 2 * 8 Gb/s Fabric Channels

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.-Nº 0636
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-229
A-

Line Cards

Two line card versions are available for the Catalyst 6000 Family. Because customers have the option of using the 32-Gbps switching bus or the 256-Gbps SFM, the two line card versions provide connectivity into the different fabrics. The following table lists the line cards and their compatibility.

Table 1 Line Card Summary

Line Card Version	Chassis Supported	Explanation
Non Fabric-enabled	Catalyst 6000 and 6500	Available since the inception of the Catalyst 6000 Family. These line cards connect to the 32-Gbps bus and can be used in all chassis.
Fabric-enabled	Catalyst 6500	Connect into both the 32-Gbps bus and the SFM. The SFM is not supported in the Catalyst 6000 Series.
Fabric-only	Catalyst 6500	Connect only to the SFM and provide the highest levels of system performance and throughput. These line cards require the SFM because they do not connect to the 32-Gbps bus.

Because the non fabric-enabled line cards can be used in any chassis option they provide the greatest flexibility and investment protection for customers who have already deployed the Catalyst 6000 Family. For customers requiring very high bandwidth and throughput, Cisco recommends using the fabric-enabled or fabric-only line cards.

Note: All line cards interoperate with each other. For example, a non fabric-enabled line card in the Catalyst 6500 interoperates with a fabric-only line card in the same system. An explanation of how that works is provided in the section titled "Catalyst 6000 Family Packet Flow—A Day in the Life of a Packet."

Supervisor Options

The Catalyst 6500 Series includes two versions of the Supervisor Engine. The Supervisor Engine is required for system operations; a chassis without a Supervisor will not operate. The Supervisor Engine uses slot 1 in the chassis. The second slot in the system, slot 2, can be used for a secondary redundant supervisor engine. Note that because of the switching implementation of the Catalyst 6000 and 6500, only one Supervisor Engine needs to be active at one time. However, with the High Availability feature enabled, both supervisors maintain the same state information, including Spanning-Tree topology, forwarding tables, and management information, so that if the primary supervisor fails, the redundant engine can take over within two seconds.

To address the needs of different customers who deploy the Catalyst 6500 in varying applications, Cisco provides two Supervisor Engines.

Supervisor Engine 1

Supervisor 1, the first switching engine for the Catalyst 6000 Family, provides performance levels of 15 million pps using a cache-based switching scheme. Supervisor 1 has three main components: the Network Management Processor (NMP), the Multilayer Switch Feature Card (MSFC) and the Policy Feature Card (PFC). Each component provides a critical function to the network.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0637
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.225
A-

Supervisor 1 is available in three options:

- Basic Layer 2 switching with no Layer 3-based QoS or security access control lists (ACLs), although port-based class of service (CoS) and destination MAC address-based CoS is supported. Basic switching based on the MAC address is supported.
- Supervisor 1 with the PFC, which provides Layer 2 switching with Layer 3 services (including QoS and security ACLs). QoS classification and queuing, as well as security filtering, is supported at data rates of 15 million pps. This functionality is supported at Layer 2 and 3 even though Layer 3 switching and routing is not performed.
- Supervisor 1 with PFC/MSFC1 (or 2), which provides full Layer 3 switching and routing. This combination enables the Catalyst 6500 to route IP and Internet Packet Exchange (IPX) traffic at 15 million pps.

Supervisor Engine 2

Supervisor Engine 2 is designed specifically for service provider and high-end enterprise core applications. This supervisor engine provides forwarding capability of up to 30 million pps when using fabric-enabled line cards and the SFM (both must be used). An important difference between the Supervisor 1 and Supervisor 2 is that Supervisor 2 supports Cisco Express Forwarding (CEF) in hardware. CEF is a switching implementation that is based on the topology of the network rather than the traffic flow. This causes the control plane of the Catalyst 6500 scale to converge faster in the event of a route flap and perform lookups for millions of flows (which occur in Internet service provider [ISP] deployments).

Supervisor 2 has two options:

- Supervisor 2 with PFC-2, which provides QoS, Private Virtual LAN (PVLAN), and ACL functionality at 30 million pps with no performance penalty.
- Supervisor 2 with PFC-2/MSFC-2, which enables full routing on the Catalyst 6500. This supervisor enables the Catalyst 6500 to provide Internet-class routing and high performance.

Supervisor Engine 2 can be used in the Catalyst 6000 and Catalyst 6500 chassis. The SFM requires use of Supervisor 2, but Supervisor 2 can operate independently of the SFM.

Catalyst 6000 Family Architecture

The Catalyst 6000 and Catalyst 6500 Series architecture is described in several sections of this paper. Each section details the system functionality and how the components operate. This section covers the following topics.

- Catalyst 6000 and 6500 switching bus architecture
- Catalyst 6500 SFM architecture
- The Multilayer Switch Feature Card (MSFC)
- Switching implementation on Supervisor 1
- Switching implementation on Supervisor 2
- Distributed Forwarding Card (DFC)
- QoS and ACL handling
- Line card buffering and ASIC overview

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0638
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

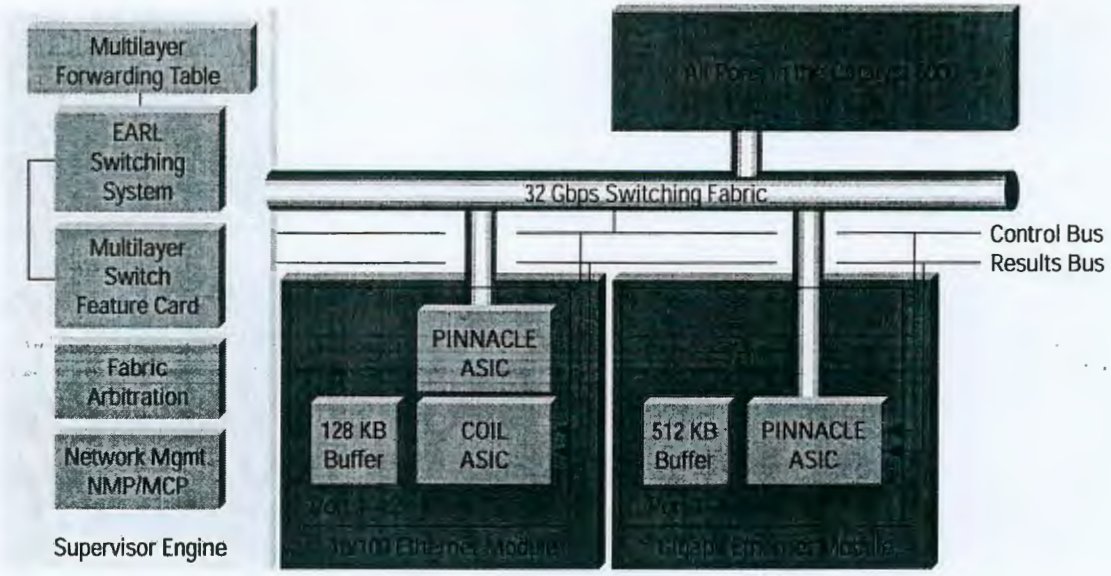
15.227
A.

The Switching Fabric—Moving the Packet

Catalyst 6000 and 6500 Switching Bus Architecture

Figure 4 illustrates the Catalyst 6000 Family architecture.

Figure 4 Catalyst 6000 and 6500 Switching Bus Architecture



The Catalyst 6000 system is based on a 32-Gbps advanced pipelining switching bus. The switching bus is a shared medium bus; that is, all the ports attached to the bus see all the frames transmitting across it. Coupled with the pipelining mechanism, this switching is very efficient because after a decision is made the switching engine orders the nondestination ports to ignore the frame.

The Catalyst 6000 switching bus includes three distinct buses: the D-bus (or Data bus), the C-bus (or Control bus), and the R-bus (or results bus). All non fabric-enabled line cards connect to the switching bus through the connectors on the right side of the chassis (see Figure 1). The D-bus is the bus where data is forwarded from one port to another and realizes a bandwidth of 32 Gbps. The Results bus (R) takes information from the switching logic located on the Supervisor Engine back to all the ports on the switch. The control bus (C-bus) relays information between the port ASICs and the Network Management Processor (NMP).

Two notable features on the switching bus of the Catalyst 6000 are pipelining and burst mode. Pipelining enables the Catalyst 6000 Family systems to switch multiple frames onto the bus before obtaining the results of the first frame. Typically, on shared medium architectures, only a single frame or packet can reside on the bus at a time. The entire lookup process by the forwarding engine happens in parallel to the transfer of the frame across the switching bus.

If the frame is switched across the switching bus before the lookup is done, the switching bus is idle until the lookup is done. This is where pipelining comes into play. Ports are allowed to source frames on the switching bus before the results of the first frame lookup are done. The second frame (from any port) is switched across the bus and pipelined for a lookup operation at the forwarding engine. Thirty-one such frames can be switched across the switching bus before the result of the first frame is received. The 32nd frame must wait before it can be sourced on the switching bus.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0639
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

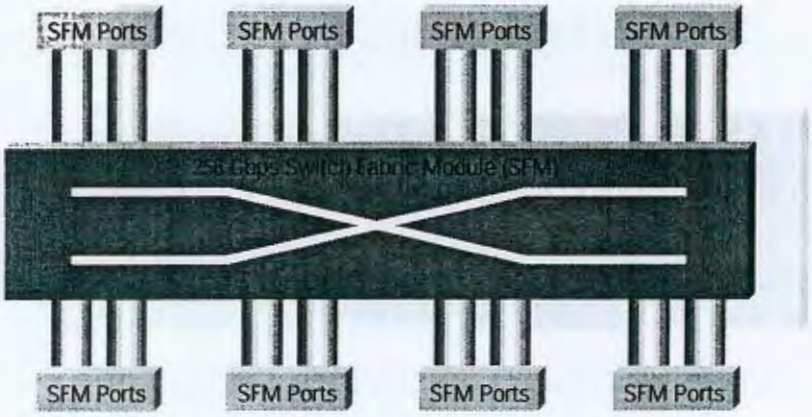
The Burst-Mode feature enables the port to source multiple frames on the switching bus. If the port sends just one frame each time it is granted access to the data bus, there is potentially an unfair allocation of bandwidth to the bus when it is heavily loaded. For example, if two ports are trying to send data and one has 100-byte frames while the other has 1000-byte frames, the port with the 1000-byte frames can switch 10 times as much data as the one with 100-byte frames. This is because they alternate in the arbitration and each sends one frame at a time.

In the Catalyst 6000 Family systems, a port can send multiple frames to the switching bus in a manner that controls the amount of bandwidth it consumes regardless of the frame size. To accomplish this, the port ASICs maintain a counter of the number of bytes it has transferred and compare it to a threshold. Provided that the count is below threshold value, the port continues to send frames as long as it has data to send. When the count exceeds the threshold, the port stops sending data after completing the current frame and stops transmitting because the arbitration logic at this point senses the condition and removes bus access. The threshold value is a function of the number of ports in the system, their thresholds, empirical data, simulation results, and so forth. The system automatically computes the threshold value to ensure fair distribution.

Catalyst 6500 Crossbar Switching Fabric

The Catalyst 6500 and the Switch Fabric Module (SFM) provide a 256-Gbps switching system with forwarding rates over 100 million pps. The SFM uses the connectors on the left side of the Catalyst 6500 chassis. Note that because these connectors are not in the Catalyst 6000, this chassis cannot use the SFM. The SFM uses a 256-Gbps crossbar switching fabric to interconnect the line cards on the switch. Figure 5 is a logical diagram of the SFM.

Figure 5 Catalyst 6500 Switch Fabric Module



The SFM can best be thought of as a 16-port "switch," with the ports actually connecting to the line cards. In the Catalyst 6500, each slot in the chassis receives two crossbar ports, and each port is clocked at 8 Gbps (the actual bandwidth is 16 Gbps because there is one 8-Gbps path for transmitting into the crossbar and 8 Gbps for transmitting out of the crossbar). The fabric-enabled modules connect to one of the ports on the crossbar, providing 8-Gbps access into the switching fabric. The fabric-only line cards attach to both ports per slot into the crossbar, allowing them 16 Gbps of connectivity.

The Catalyst 6500 SFM uses overspeed to eliminate congestion and head-of-line blocking. Overspeed is a concept by which the internal "paths" *within* the crossbar fabric are clocked at a speed faster than the input rates *into* the crossbar. This allows packets to be switched out of the source module through the fabric to the output line card at high data rates. The SFM uses 3x overspeed, meaning that each internal trace is clocked at 24 Gbps relative to the input rate, which is clocked at 8 Gbps.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0640
3690
Doc.

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.225
A-

Local Switching on the Fabric-Enabled Line Cards

Each of the line cards connecting to the SFM uses a local switching fabric. The fabric-enabled cards, such as the WS-X6516, support the DFC to enable high-speed switching. These line cards have connectivity to one channel port on the SFM and also have a connection into the 32-Gbps centralized switching bus. The fabric-only line cards, such as the WS-X6816, connect only into the SFM via dual fabric channels. Figure 6 and Figure 7 show these line cards.

Figure 6 SFM Single-Attached Fabric-Enabled Card with Optional DFC

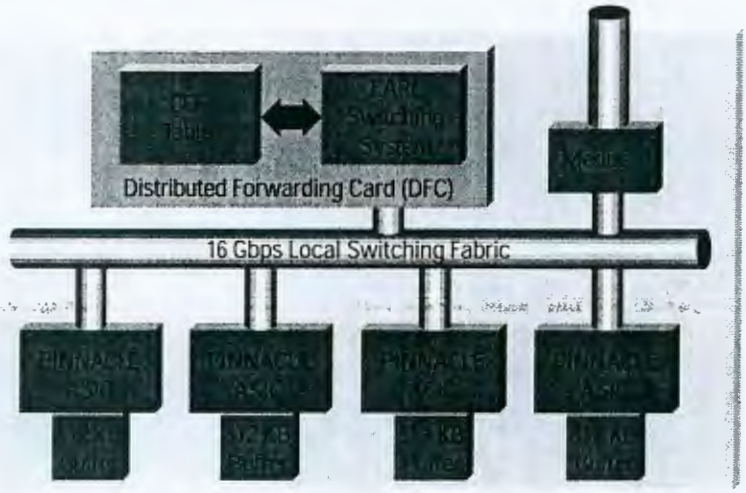
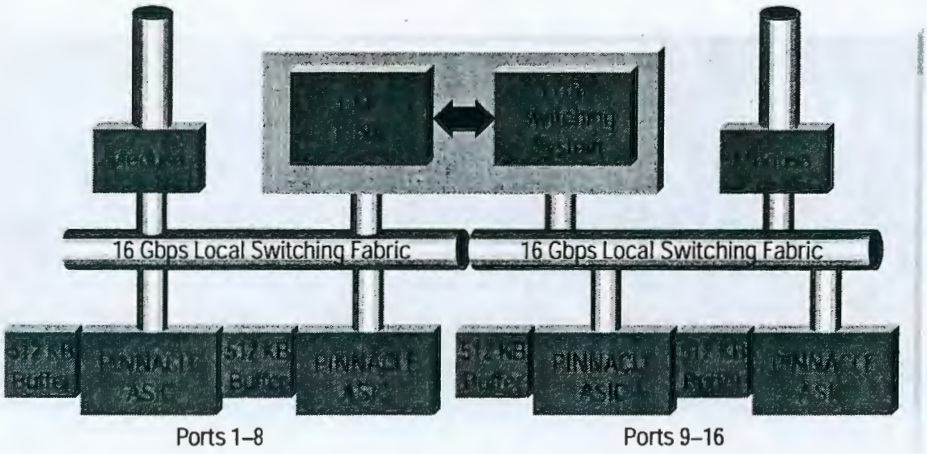


Figure 7 SFM Fabric-only Line Cards



The key difference between the two line cards is that the fabric-enabled cards use a single local switching bus with a bandwidth capacity of 16 Gbps. The fabric-only line cards use two local switching buses, each clocked at 16 Gbps. Both line cards can support distributed forwarding. The DFC daughter card is available as an add-on for the fabric-enabled cards. The fabric-only line cards have the DFC embedded in the system.

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 0641
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-224
4-

A critical component of the local-switch implementation is the connection point between the local system and the SFM. In the Catalyst 6500, this function is handled by an ASIC called Medusa. This ASIC is the interface between the local bus and the crossbar. On the fabric-enabled cards (*not* the fabric-only cards), Medusa also interfaces to the main 32-Gbps switching bus. How Medusa actually functions in packet switching is discussed in a later section titled "Catalyst 6000 Family Packet Flow—A Day in the Life of a Packet".

The Switching Implementation—Making a Switching Decision

Switching implementations use two key functions: the control plane and the data-forwarding plane. The control plane maintains all of the overhead functions of the switch, including handling of the routing protocols, the routing table, flow initiation, and some access control. This function, often overlooked in the "race for speed," is absolutely critical to the switching architecture and cannot be ignored. In the Catalyst 6000 Family, the MSFC handles the control plane function. The packet forwarding decision is done in hardware and can take place at data rates exceeding 100 million pps. This functionality is handled by the Supervisor Engines and, on some line cards, the Distributed Forwarding Cards (DFCs).

Multilayer Switch Feature Card (MSFC)

The Catalyst 6500 uses centralized routing control plane functionality. This capability is provided by a daughter card module called the MSFC on the Supervisor Engine. The MSFC handles all of the control plane functions within the switch architecture.

Note: There are two versions of the MSFC: MSFC-1 and MSFC-2. This document focuses on the MSFC-2.

The MSFC is based on an R7000 300-MHz processor. This gives the MSFC a forwarding performance rate in software of 650,000 pps. For a Catalyst 6500 using Supervisor Engine 1, this provides very high performance for the flow setup, which the architecture mandates.

The MSFC can handle and maintain large routing tables. There are three memory options available: the standard 128 Mbytes, an option for 256 MB, and an option for 512 MB. For networks that require the Catalyst 6500 to handle the entire Internet routing table, Cisco recommends the 512 MB version.

For Supervisor Engines 1 and 2, the MSFC maintains the routing table and communicates across an out-of-band bus to the hardware switching ASICs. On Supervisor Engine 1, the first packet in a flow that does not have an entry in the hardware-switching table is sent to the MSFC for software processing. The MSFC compares the destination IP address with the routing table and make a forwarding decision. After the MSFC has switched the first packet of a new flow in software, the hardware is automatically programmed to switch subsequent packets in the ASIC complex.

In Supervisor Engine 2, the MSFC does not forward IP frames. Instead, it builds a CEF table (also known as a Forwarding Information Base [FIB]) table, which is based on the contents of the routing table. The CEF table contains the same information as the routing table and uses a highly optimized search algorithm in order to "hit" on the destination network. The MSFC downloads the CEF table directly into the hardware so all packets are switched in hardware and not by the MSFC itself.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0642
Doc. 3690

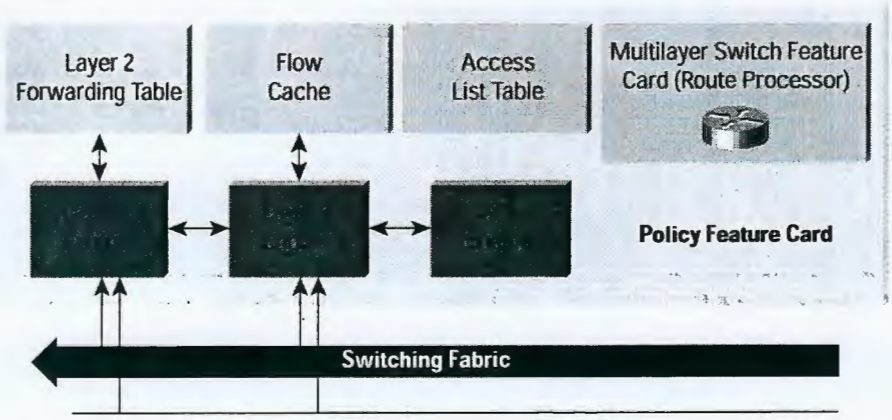
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-223
JA-

Supervisor Engine 1A and the Policy Feature Card—Traffic-based Switching

The second critical component of switching in the Catalyst 6000 Family also resides on the Supervisor engine and is called the Policy Feature Card (PFC). The PFC actually contains the switching ASICs that enable high-speed switch at data rates up to 15 million pps. Because there are substantial differences between Supervisor Engine 1 and Supervisor Engine 2, these differences are addressed separately. The following figure shows the functional components of the PFC.

Figure 8 Supervisor 1 and the Policy Feature Card



The PFC is the heart of the switching system. The forwarding decisions of the Catalyst 6500 are made by three ASICs: one for Layer 2 MAC-based forwarding, one for Layer 3, and the other for ACLs, whether for security or QoS. The Layer 2 ASIC handles two key items. First, and somewhat obviously, it looks up MAC addresses within a broadcast domain in order to switch at Layer 2. However, this ASIC also identifies a packet (or flow) that needs to be Layer 3 switched. The MSFC, shown in the figure above, primes an entry in the flow cache, which the Layer 3 engine uses to switch packets in hardware. The MSFC registers its MAC address with the Layer 2 Engine, so that, upon examination of a packet, the Layer 2 engine can decide to ignore the result of the lookup performed by the Layer 3 engine.

After the system determines that Layer 3 switching needs to take place, the result of the Layer 3 engine is used. The Catalyst 6500 with a Supervisor 1 uses a switching mechanism called traffic-based switching (also known as flow-caching). A flow is defined as a traffic stream from a source IP address to a destination IP address. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port information can also be stored as part of the flow cache entry. When the first packet in a flow enters the switch, a lookup is done in the hardware lookup table to see if an entry exists. If one does not, the packet is sent to the routing software running on the switch's CPU, which matches the destination IP address against the routing table, locates VLAN-of-exit, switches the packet, and automatically creates an entry in the hardware flow-cache. Subsequent packets can be switched in hardware. For this system to work effectively, a fast CPU, and more importantly, fast and efficient software, must be used.

The Catalyst 6500 flow cache can support a maximum of 128,000 entries. How the flow cache is used depends on how the Catalyst 6500 is "told" by the network manager to switch flows (the command line interface allows this configuration). There are three options in the Catalyst 6500.

- Destination-only—In this case, a flow is built and stored in the PFC based on the destination IP address. This allows for the best utilization of the PFC flow cache as multiple sources communicating with one destination IP address (a server, for example) only use a single flow entry.
- Source-destination—In this case, a flow is built based on both the source and the destination address. This takes up more entries in the cache if, for example, five sources are talking with one destination, that uses five entries in the cache.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0643
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Full flow—This is a very expensive way of using the flow cache. In this mechanism, a flow is created on not only the source and destination IP, but also on the UDP or TCP port number. A single IP source and destination pair could potentially take up several entries, one for each TCP or UDP stream.

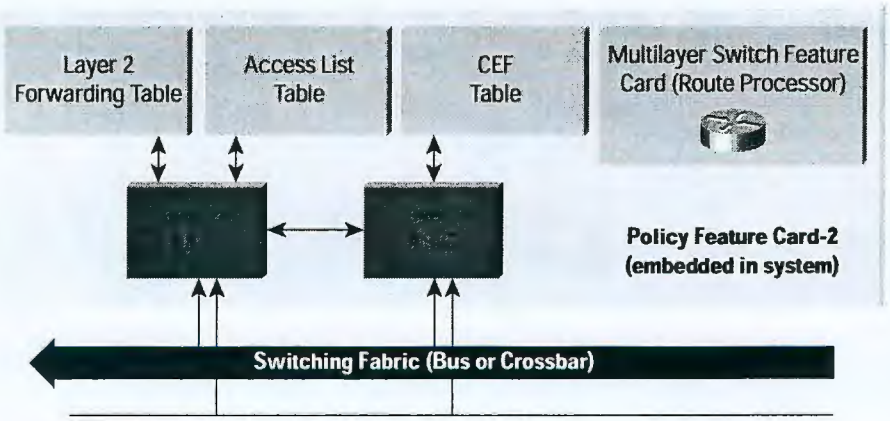
The flow table is broken up into 8 pages of memory; each page can store 16,000 entries. A hashing algorithm is used to perform lookups in the table. The hashing algorithm is critical both to learning packets and storing them at high speed as well as switching at data rates of 15 million pps. Because of the statistical nature of hashing algorithms, hash collisions can occur. A hash collision occurs when the lookup for two packets hashes to the same location in memory. To account for this, the Layer 3 engine turns to the next page in memory to see if that location is used. This will continue either until the address is learned or until the eighth page is reached. If the learning information still cannot be stored, then the packet is flooded (at Layer 2) or sent to the MSFC (for Layer 3). Note that, since network are very dynamic, with flows being learned and aged out, that this is a very rare occurrence.

The Supervisor Engine 1 with the PFC is designed to forward packets at 15 million pps. Cisco recommends it for deployment in most network scenarios, including the network access layer (such as a wiring closet or server farm) and enterprise network distribution points (such as the MDF of a large building).

Supervisor Engine 2—CEF-based Forwarding in Hardware

Supervisor Engine 2 for the Catalyst 6500 provides higher speed switching and resiliency relative to Supervisor Engine 1. The switching system on Supervisor 2, often referred to as PFC-2, can provide data rates up to 30 million pps. The major difference in the system is the switching implementation. Unlike Supervisor 1A, Supervisor 2 uses a CEF-based forwarding system in hardware. The following figure illustrates the PFC-2 on Supervisor Engine 2.

Figure 9 Policy Feature Card 2 on Supervisor Engine 2



There are several differences in PFC-2. The most noticeable one is the combination of the Layer 2 and ACL engines into a single engine. Also important is the fact that a flow cache is no longer used in the system. The MSFC, located on Supervisor 2, downloads the CEF table to the Layer 3 engine, which in turn places the CEF table in hardware. Note that a flow cache table is also built in the PFC-2, although it is used for statistics gathering and not for packet switching.

Unlike a flow cache, which is based on traffic flow, the CEF table is based on the network topology. When a packet enters the switch, the switch performs a longest match lookup based on the destination network and the most specific netmask. Instead, for example, of switching based on a destination address of 172.34.10.3, the PFC-2 looks for the network 172.34.10.0/24 and switches to the interface connecting to that network. This scheme is highly efficient and does not involve the software for anything other than the routing table and prepopulation of the FIB table. In addition, cache invalidation because of a route flap does not occur; as soon as a change is made in the routing table, the CEF is updated immediately. This makes the CEF table more resilient to changes in the network topology.

15.222-A
CPMI - CORREIOS
Fls. Nº 0644
Doc. 3690

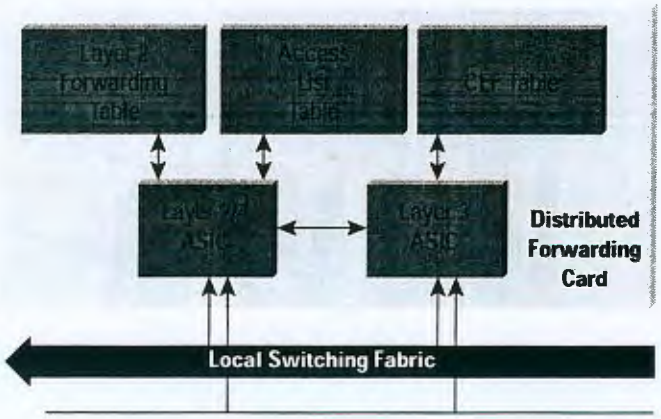
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.221
A.

Supervisor 2 can also enable distributed switching through the DFCs, which are daughter cards for the fabric-enabled line cards (such as the WS-X6516). To achieve 30 million pps, the Supervisor Engine 2 uses the 32-Gbps switching bus for control traffic from the source line card to the PFC-2. By compressing the header required for the lookup and sending it across the switching bus, the PFC-2 can look up packets much faster. The data forwarding actually takes place over the SFM. By using the DFCs, the forwarding decision is localized to the line card and, instead of sending the headers to the Supervisor Engine, the packet can be switched directly over the SFM.

Conceptually, the DFC looks the same as the PFC-2 on the Supervisor Engine. It contains virtually the same components with one exception: the routing engine (which maintains the routing table) is not present. Therefore, although the forwarding decision is localized, the control plane is still centralized. This provides the best of both worlds: centralized device control and high-speed packet forwarding. The following figure illustrates the DFC.

Figure 10 Distributed Forwarding Card Architecture



The key difference in the DFC-enabled system is that a switching decision is made on the input module instead of centrally at the Supervisor Engine. The CEF table used for switching, however, is still calculated centrally at the Supervisor Engine and then downloaded to the CEF table local to the line card. Therefore, the Supervisor CEF table and the local CEF tables are always synchronized.

The distributed nature of the Catalyst 6500 with Supervisor Engine 2 and the DFC daughter cards enables forwarding rates exceeding 100 million pps.

The Supervisor Engine 2 and the DFCs are intended for very large enterprise and service provider backbone networks. These networks, more often than not, can take advantage of the high-speed switching capability of more than 100 million pps and the resilience and scalability of CEF-based forwarding.

Quality of Service and Security Access Control Lists

The Catalyst 6500 system uses a unique mechanism for handling QoS and security ACLs in hardware. This mechanism, called Ternary CAMs (TCAMs), is used on Supervisor 1, Supervisor 2, and the DFCs. Following is a brief explanation of TCAMs and how they operate.

The PFC switching system can support up to 512 ACL labels. This switching system can identify 512 unique ACLs (by names) where each ACL can have multiple access control entry (or ACE) for a total of 32,000 maximum ACEs across 512 ACLs. The TCAM has the capability of storing 64,000 entries. This is broken up into four main blocks: input checking and output checking for QoS ACLs and input and output checking for security ACLs. Within these sections, there is a further distinction made between QoS and security ACLs.

ECT 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0645
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The operation of a TCAM is similar to a hashing table, but in the TCAM, the "hashing value" is the mask. Out of the 32K possible locations, each set of eight locations has a mask associated with it. When an access control entry (or ACE) is configured, a mask in the command syntax tells the ASIC which bits to check for in the 134-bit long flow label. Suppose the ACE has a mask, that instructs it to check for the first 20 bits, and the rest of the bits are designated "don't care" (meaning they can be any value). This results in a specific checking pattern that falls into, for example, Mask # 1.

In this example, the next time an ACE is entered that has the same mask, it will be populated as ACE 2 (if that location is available) and the process continues. If an ACE is entered that says to check for some other combination of 0, 1 or Don't Care bits, this will become Mask # 2. All ACEs matching this mask will now go in this bank, if you will. So, if every entry (flow label) in the TCAM has a different mask then a single TCAM will be able to hold 1K entries only, because there is a single mask for every eight entries.

On the other hand, if flow labels have maximum sharing of masks then we will be able to use the entire 32K within the TCAMs. This sharing of mask dictates the total number of entries that can be stored in the TCAM. Worst case is 4K entries (shared between Security ACLs and QoS) and best case is 32K.

Table 2 Example Showing TCAM Usage with Mask Sharing

ACE 1	ACE 9	ACE 17	ACE 22	ACE 30
ACE 2	ACE 10	ACE 18	ACE 23	ACE 31
ACE 3	ACE 11	ACE 19	ACE 24	ACE 32
ACE 4	ACE 12	ACE 20	ACE 25	ACE 33
ACE 5	ACE 13	ACE 51	ACE 26	Blank
ACE 6	ACE 14	Empty	ACE 27	Empty
ACE 7	ACE 15	Empty	ACE 28	Empty
ACE 8	ACE 16	Empty	ACE 29	Empty
MASK # 1	**MASK # 2**	**MASK # 3**	**MASK # 4**	**MASK # 5**

The TCAM implementation and behavior is similar for PFC-1 and PFC-2. This functionality allows for ACL lookups to take place at data rates up to 15 million pps on Supervisor Engine 1 and 30 million pps on the DFC and Supervisor Engine 2. Because ACL lookups happen in parallel to the Layer 2 and 3 lookups, there is no performance loss when using security or QoS ACLs.

Buffering and Congestion Management for the 10/100 and Gigabit Ethernet Line Cards

Buffering and congestion management are a critical component of a switching architecture. In almost every network design and architecture, there is a congestion point somewhere in the switch. Unlike many vendor's claims, that congestion point is almost never the switching fabric in a real network. Instead, the congestion point is typically an outgoing port or interface. This is seen in network designs such as in the access layer, where multiple user ports are accessing the uplink, multiple distribution switches are accessing the port to the core, and the core network aggregating traffic to the server farm, WAN, or the Internet.

The Catalyst 6500 has built the congestion management techniques into custom ASICs. These ASICs also serve to provide access from the ports onto the 32-Gbps main switching bus or the 16 Gbps local bus on the fabric-enabled and fabric-only line cards. These ASICs are also informed by the PFC (or the DFC) how to queue a packet for quality of service. There are two types of port ASICs, one for Gigabit Ethernet, the other for 10/100.

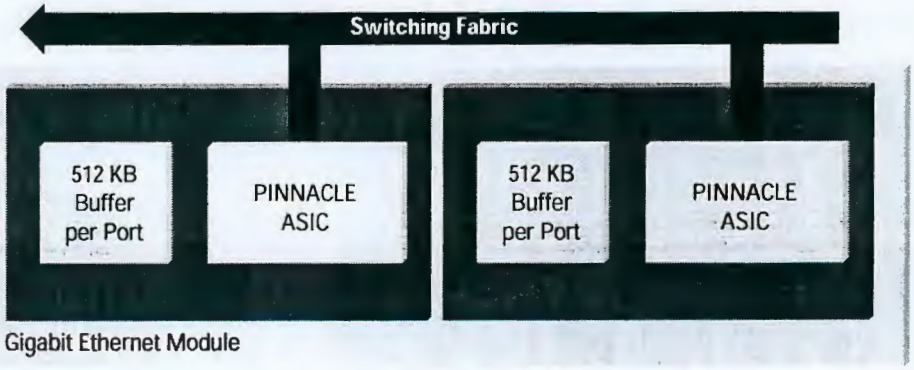
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0646
Doc 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.219
A.

The subsystem used for the Gigabit Ethernet ports is referred to as Pinnacle. A diagram of Pinnacle is shown in the figure below. Each Pinnacle ASIC controls four Gigabit Ethernet ports. On the 16-port Gigabit Ethernet line card, for example, there are four Pinnacle ASICs. Each Pinnacle ASIC maintains a 512-K buffer per port. To avoid head-of-line blocking to the switching fabric, a minimal amount of buffer is provided for the receive (or RX) queue, which is taking frames coming in from the network. The bulk of the buffering is allocated for the transmit (or TX) queue. The ratio between transmit and receive queues is 7-to-1; this means that, on each port, there is 448 Kbytes of TX buffer compared to 64 Kbytes of RX buffer. This makes the Catalyst 6500 an outbound queuing model switch.

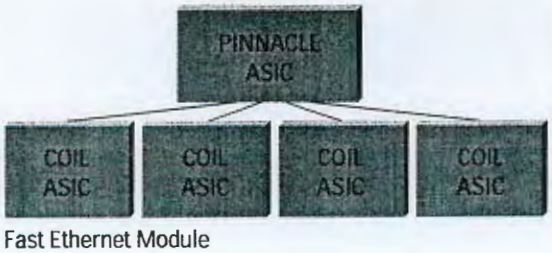
Figure 11 PINNACLE Port ASIC and Buffering



The Pinnacle ASIC takes the division of buffering a step further in regards to its handling of QoS. Each port has two receive queues and three transmit queues. Of the three TX queues, one is handled in a strict priority fashion, meaning that it always has a fixed amount of bandwidth guaranteed by the outbound scheduling logic. The other two queues are handled via the weighted round robin (WRR) scheduler. In the WRR scheduling mechanism, the two queues are weighted relative to each other and given proportional access to the outgoing port. The TX queues themselves are, by default, allocated 15 percent for strict priority, 15 percent for high priority, and 70 percent for low priority. A common example used to explain the proportion is the airline model: most of the seats are economy class, analogous to a high amount of low priority traffic; many fewer seats for business, or high priority traffic, and still fewer for first or premium class.

The 10/100 ports have a slightly different mechanism for handling congestion management. These line cards use a combination of Coil and Pinnacle to achieve congestion management. As shown in the figure below, each Coil ASIC supports 12 10/100 ports. In turn, each Pinnacle ASIC supports four COILs. This allows support for all 48 ports on the line card. Like he Gigabit Ethernet line card, COIL provides support for buffering on a per-port basis. Each 10/100 port in the system has 128 Kbytes of buffer. This buffer is broken down into a 7-to-1 ratio between TX and RX. This eliminates any head-of-line-blocking issues because of outbound interface congestion.

Figure 12 COIL ASIC Configuration on 10/100 Line Cards



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1849
Doc. 3690

Congestion management is an important system consideration within the architecture. The ability of the switch to handle situations of many-to-one traffic flows is key to ensuring that the architecture will perform in a real network.

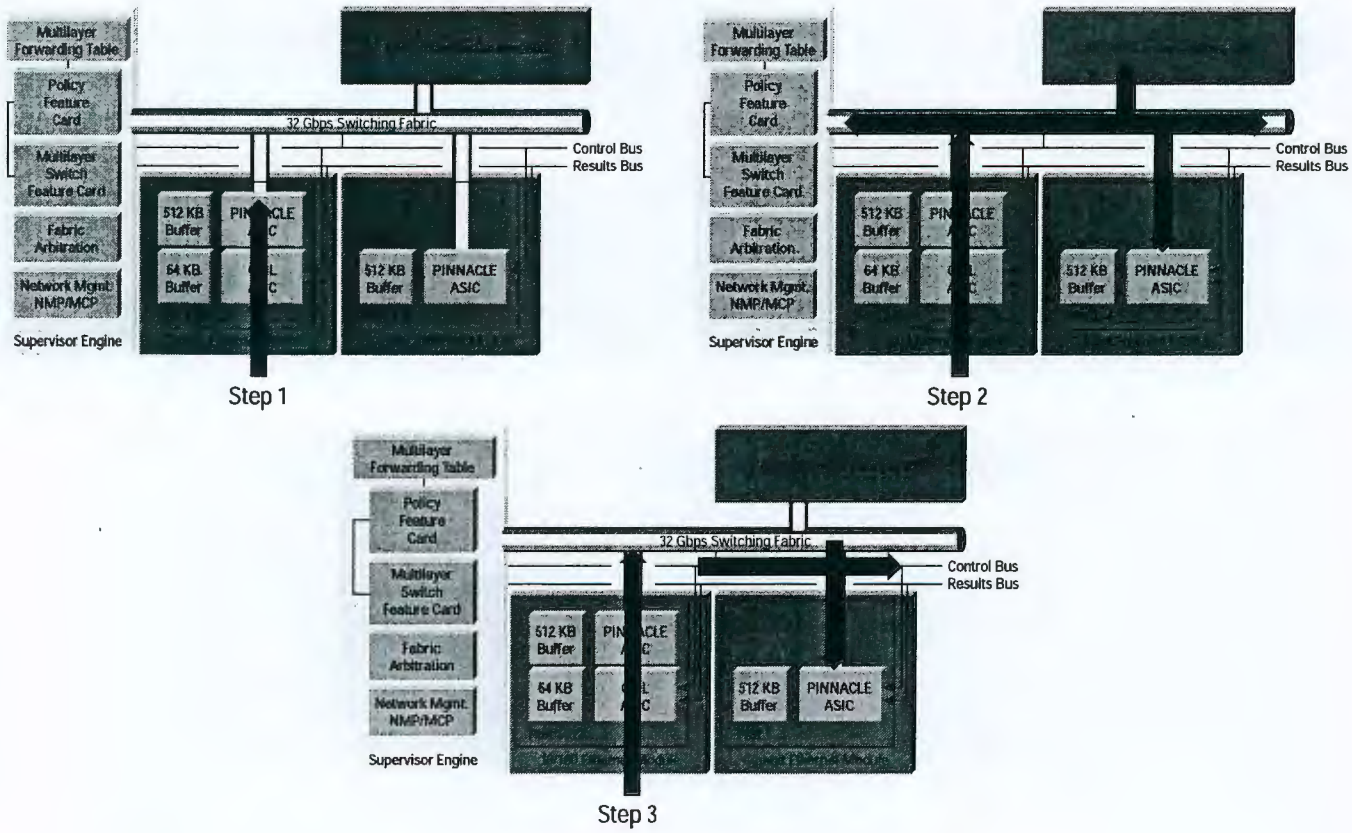
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Catalyst 6000 Family Packet Flow—"A Day in the Life of a Packet"

Catalyst 6000 and the 32-Gbps Switching Bus

This section details how packets actually flow through the switch. Refer to the diagram below for a step-by-step process.

Figure 13 Catalyst 6000 and the 32-Gbps Switching Bus Packet Switching



Step 1—Packet enters the switch

When a frame enters the Catalyst 6000 switch, the input port takes the frame in and places it in the input buffer. The input buffer is design to handle store-and-forward checking and hold the frame while PINNACLE arbitrates for access onto the switching bus. There is a local arbiter on each line card that is responsible for allowing each port on each PINNACLE access to the switching bus. This local arbiter signals the central arbiter (on the Supervisor Engine), which is responsible for allowing each local arbiter to allow frames onto the switching bus.

Step 2—Packet sent across switching fabric and lookup takes place

The switching bus on the Catalyst 6000 is a shared medium, meaning that all the ports on the switch see the packet as it is on the bus. Once the central arbiter has granted access to the switching fabric, the packet is sent across the bus. All ports begin downloading that packet into their transmit buffers. The PFC is also looking at the switching bus, sees the frame and initiates a lookup. First, the Layer 2 table is consulted. If the packet is local to the VLAN, a switching decision is finished. If the Layer 2 table is the router's MAC address, then the Layer 3 engine examines the packet and determines if a forwarding entry exists in hardware. If not, the packet is sent to the MSFC. If an entry does exist, the destination VLAN is identified and the Layer 2 lookup table is consulted again, this time to determine the MAC address within the VLAN and is associated outbound port.

15.213
RQS nº 03/2005 - CN
CPMI - CORREIOS
0648
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.217
A-

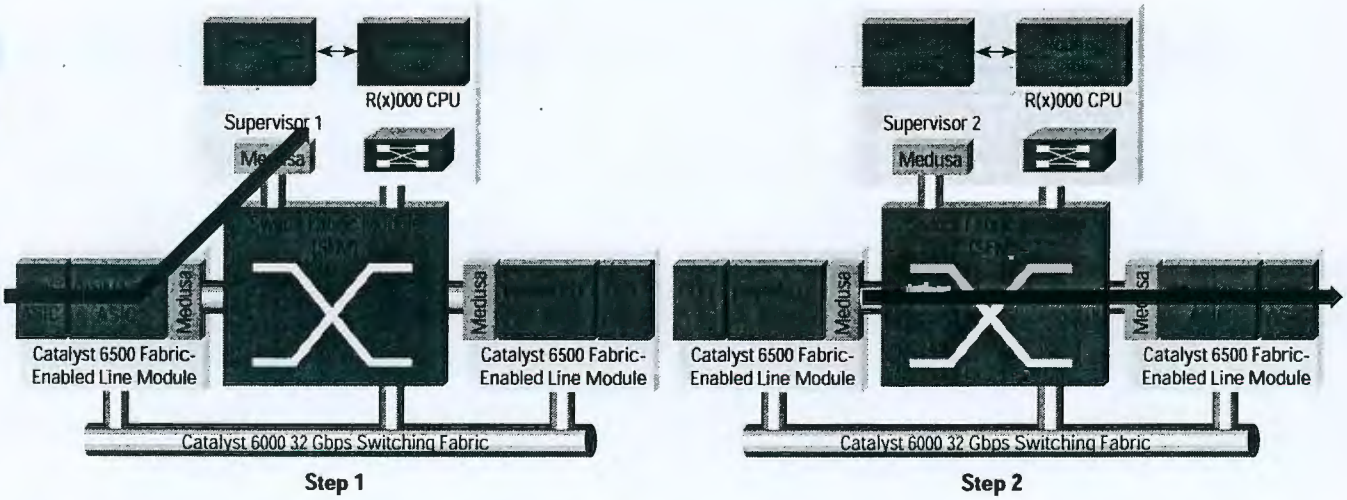
Step 3—Forwarding the packet

Now that the outgoing interface has been identified, all the ports on the switch that are not the destination port are told, over the Results Bus, to flush their buffers of that packet. The Results Bus also carries to the destination port the MAC re-write information and the appropriate QoS parameters to use (so the packet can be queued correctly on the outgoing port). Once the destination port has received the packet, PINNACLE queues the packet in the correct queue and then uses the SP/WRR scheduler to switch the frame out of memory to the destination external to the switch.

Catalyst 6500 and the SFM with Centralized Switching

This section details how packets actually flow through the Catalyst 6500 equipped with the Switch Fabric Module. Refer to the diagram below for a step-by-step process.

Figure 14 Catalyst 6000 and the SFM with Centralized Switching Packet Flow



Step 1a—Handling the frame on the local line card.

A fabric-enabled system is different from the Catalyst 6000 bus-based system, however, there are remarkable similarities. Each SFM-enabled line card can be thought of conceptually as a Catalyst 6000 on a line card. The switching functionality, therefore, is fairly similar. The packet first enters the switch and its handled by PINNACLE the same way as in the Catalyst 6000 system. Arbitration is required on the local 16 Gbps bus and, while the packet is on the local bus, the header information required for look-up is parsed by the Medusa ASIC, compressed, and sent across the 32-Gbps bus to the Supervisor Engine. All of the Medusa ASICs on all the line cards see that frame and download the information.

Step 1b—Packet Lookup.

The packet is received by Supervisor Engine 2 and is presented to the PFC-2, which includes both the Layer 2 and 3 forwarding tables. Like PFC-1, a Layer 2 lookup is performed to determine whether a Layer 3 switching decision needs to be made. If a Layer 3 decision is needed, the header information is looked up by the Layer 3 engine, which is utilizing the CEF table. Once a destination VLAN is identified, a second Layer 2 lookup is performed to determine the correct MAC address. This information is then sent across the results bus, which, again, all line cards Medusas see. All Medusas except the destination drop the frame from its buffers.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0649
Doc 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

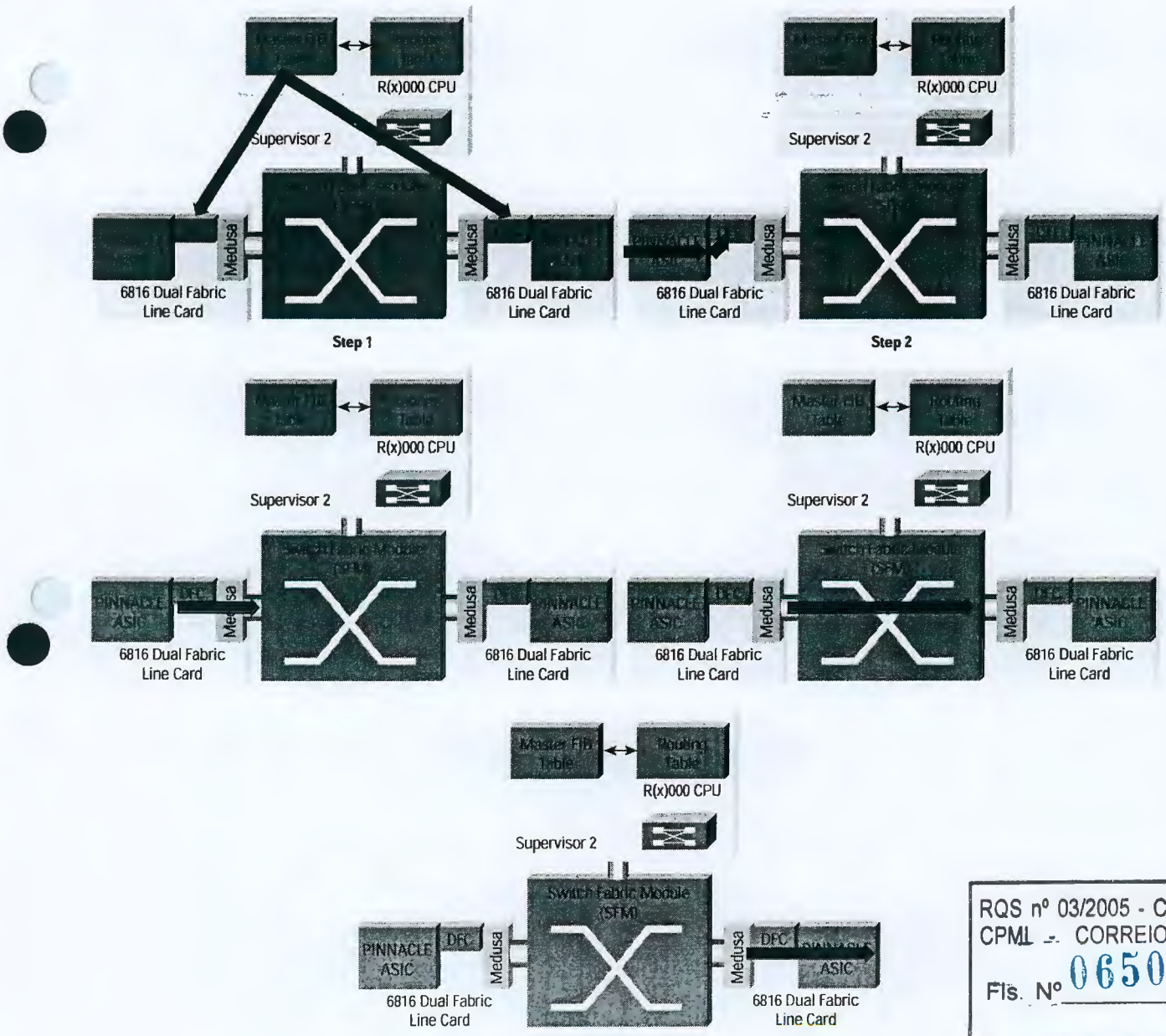
Step 2—Forwarding the packet.

The source line card now knows where the destination is. The line card, via the crossbar interface, adds a tag, which identifies the destination line card and sends the packet into the SFM. The SFM switches the frame to the appropriate destination line card. The information on the Results bus informs the destination line card what the destination port is and what the port of exit is. The packet is queued, for QoS, the same way it is in the Catalyst 6000 system. The WRR scheduler then sends the frame out to the network.

Catalyst 6500 and the SFM with Distributed Switching

This section details how packets flow through the Catalyst 6500 equipped with the SFM and distributed switching. Refer to the following diagram for a step-by-step process.

Figure 15 Distributed Forwarding Packet Switching



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0650
Doc. 3690

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.215
A.

Step 1—Downloading the CEF table

The first step in the distributed switching model of the Catalyst 6500 is to calculate the CEF table and download that to the line cards. As stated earlier in this paper, the CEF table is calculated based on the entries in the routing table. This table is computed centrally at the MSFC-2 on the Supervisor Engine and downloaded to the PFC-2 and DFC (or integrated CEF table). Therefore, the local and central CEF tables contain the same information.

Step 2—Packet lookups

When a packet enters the switch, it is handled by PINNACLE and arbitration is requested for the local switching bus. All ports on the local bus see that frame, including the DFC. The DFC performs a lookup in the local table and identifies whether the destination is local to the line card or across the switching fabric.

Step 3—Switching the packet to the SFM

If the destination is across the SFM, the DFC tells the SFM interface controller (called Medusa) to prepend a tag on the packet identifying the exit "port" on the SFM.

tep 4—Packet switching in the SFM

Once the packet is received by the SFM, the SFM examines the tag prepended to the packet and makes its own switching decision. Remember that the fabric uses 3x overspeed, so, although the inputs to the SFM is 8 Gbps, internal switching takes place at 24 Gbps. The SFM identifies the outgoing port and switches the frame to the Medusa ASIC on the outgoing line card.

Step 5—Switching the frame to the outbound port

The Medusa on the outgoing port takes the frame out of the SFM and places it on the switching bus. Since a switching decision has already been made, the local data bus and results bus are driven with data at the same time. The data bus broadcasts the frame and the results bus indicates what the destination port is. The information on the Results bus informs the destination line card what the destination port is and what the port of exit is. The packet is queued, for QoS, the same way it is in the Catalyst 6000 system. The WRR scheduler then sends the frame out to the network.

Conclusion

The Catalyst 6000 Family, including the Catalyst 6000 and 6500, is an advanced multilayer switching system capable of switching at speeds of more than 100 million pps. Subsequent documents will review the actual performance capabilities ested and verified in the lab. By incorporating Layer 2–4 capabilities in hardware, the system delivers high performance, superior functionality, and high availability to enterprise and service provider networks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0651
Doc. 3690

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.214
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0652
Doc. 3690

15.013
CA

Cisco Systems

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

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Asia Pacific Headquarters
Cisco Systems 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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Printed in the USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0353
Doc. 3690

15.212
A

Switch Tipo 1 doc 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0654
Doc. 3690

Catalyst 6000 Family — Multilayer Switches

15.215
A

Product Overview

The Catalyst 6000 Family—consisting of the Catalyst 6500 series and the Catalyst 6000 series - delivers a family of high-performance, multilayer switching solutions for Enterprise and Service Provider networks. Designed to address the increased requirements for gigabit scalability, data and voice integration, LAN/WAN/MAN convergence, high-availability, and multilayer switching in backbone/distribution and server-aggregation environments, the Catalyst 6000 Family complements the Catalyst 5000 Family and 8500 Series switches, which continue to provide premier wiring closet and network-core solutions, respectively. Together, the Catalyst Family delivers a wide range of intelligent solutions, enabling internet/intranets for multicast, mission-critical, and voice applications.

The Catalyst 6000 Family delivers exceptional scalability and price/performance, supporting a wide range of interface densities, performance, and high-availability options. Its application intelligence and quality-of-service mechanisms enable customers to effectively leverage their network for increased mission-critical applications, such as multicast and ERP, without sacrificing network performance. Coupled with the extensive network services of Cisco IOS, the Catalyst 6000 Family delivers powerful management, user mobility, security, high-availability, and multimedia support required for today's networks.

The Catalyst 6000 Family consists of the Catalyst 6000 Series and the Catalyst 6500 Series. A six-slot chassis and a nine-slot chassis are available in both the Catalyst 6000 and 6500 series. In addition, the Catalyst 6500 series also supports a chassis with nine vertical slots (WS-C6509-NEB) as well as a 13-slot chassis (WS-C6513) providing a wide range of configuration and price/performance options.

Designed for Network Equipment Building Systems (NEBS) Level 3 compliance, the nine-slot vertical chassis has back-to-front airflow and is ideally suited for service-provider environments. It is also suitable for those enterprise customer environments in which front-to-back airflow is preferred.

The 13-slot chassis, the latest addition to the chassis family, is ideally suited for high performance, high port density Fast Ethernet and Gigabit Ethernet aggregation in all parts of the network including the access, distribution, and backbone layers as well as the server farm and data center environments. With up to 12 payload slots available, the 13-slot chassis offers industry leading 10/100 and Gigabit Ethernet port densities while providing unsurpassed levels of network resilience.

Both Catalyst 6000 and 6500 Series switches support a wide range of interface types and densities, to include support for up to 576 10/100 Ethernet, 288 100FX Fast Ethernet, 12 OC12 ATM, and up to 194 Gigabit Ethernet ports - the highest in the industry. The architecture of the Catalyst 6500 Series supports scalable switching bandwidth up to 256 Gbps and scalable multilayer switching up to 210 Mpps. For customers not requiring the performance of the Catalyst 6500 Series, the Catalyst 6000 Series provides a more cost-effective solution, delivering backplane bandwidth of 32 Gbps and multilayer switching up to 30 Mpps. For investment protection, both series support the same suite of supervisors, interface line cards, and common equipment providing a wide range of price/performance options.

Key Features and Benefits

- Scalable platforms, ranging from the Catalyst 6000 Series which offers 32 Gbps of switching capacity and scalable multilayer switching up to 30 Mpps, to the Catalyst 6500 Series offering scalable switching capacity up to 256 Gbps and multilayer switching up to 210 Mpps
- Modular chassis within both Catalyst 6000 and 6500 Series, offering slot densities of 6- and 9-slot systems. In addition, a 13-slot system is also available in the Catalyst 6500 Series. Catalyst 6006, 6009, 6506, 6509, and 6513 support a wide range of configuration and price/performance options. Both switches series support the same suite of supervisors, interface line cards, and common equipment, easing sparing requirements and protecting investments with upward performance migration
- Supports a wide range of interface types and densities, to include support for up to 576 10/100 Ethernet, 288 100FX Fast Ethernet, 194 gigabit Ethernet, and twelve 10 Gigabit Ethernet ports.
- MultiLayer Switch Feature Card (MSFC) available for wire-rate IP, IPX and IP-multicast routing support, as well as support for AppleTalk, DecNet, and Vines; MSFC also supports web-caching techniques for cost-effective web-scaling
- Transceiver flexibility is supported on all gigabit Ethernet ports, such that interface requirement changes do not require a new module, but can be satisfied by a simple GBIC change

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0655
Doc. 3690

- Supports up to 8 physical Fast Ethernet, Gigabit Ethernet or 10 Gigabit Ethernet links using either Fast EtherChannel (FEC), Gigabit EtherChannel (GEC), or 10 Gigabit EtherChannel (10GEC), respectively, for logical connections up to 160 Gbps. EtherChannel ports can also be aggregated across modules for even higher-availability connectivity.
- Leverages the software and management infrastructure of the Catalyst Family, providing industry-leading services based upon Cisco Internetwork Operating System (Cisco IOS). Cisco IOS delivers a full suite of software services responsible for managing network security, allocating and enforcing quality of service, and providing value-added services enabling high network resiliency. Cisco IOS also provides the management framework for CiscoWorks2000 and Cisco Resource Essentials.
- Efficient intranet multimedia and multicast support through Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Cisco Group Management Protocol (CGMP), and GARP Multicast Registration Protocol (GMRP) deliver end-to-end, scalable bandwidth for multimedia and multicast applications
- Policy Feature Card (PFC) available for wire-rate traffic detection and classification, admission control, and access list; also supports Accelerated Server Load-Balancing in conjunction with Cisco Local Director intelligence.
- Extensive Quality of Service (QoS) support through use of Layer-2/3/4 information such as precedence bits from IP, Cisco's ISL, and 802.1p frames or Layer-4 port numbers. Support for multiple queues with configurable thresholds, and ToS/CoS-mapping mechanisms to insure that QoS is maintained as packets traverse Layer-2/Layer-3 boundaries. Resource Reservation Protocol (RSVP) priority mapping also used, ensuring timely delivery of time-sensitive intranet applications
- Support for a broad range of Cisco IOS-based security mechanisms such as port filtering, enabling individual ports to allow access only to certain workstations. TACACS+ and IP permit lists prevent unauthorized access to the switch in secure management environments. Access control lists (ACLs) secure networks from unauthorized users. MD5 Route Authentication is also used to prevent fraudulent routing updates
- Support for Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and dynamic VLAN services for optimal, scalable performance, and easing moves, adds and changes
- Support for multiple levels of network resiliency and serviceability. Device-level fault tolerance, to include the following options:
  - —Redundant Supervisors
  - —Redundant Load-Sharing Power Supplies (AC & DC)
  - —Redundant Load-Sharing Fans
  - —Redundant System Clocks
  - —Redundant Uplinks
  - —Redundant Switch Fabrics (Catalyst 6500 Series only)

All system elements including power supplies, fans, supervisors, line-card modules, and switch fabrics are hot-swappable such that elements can be added, removed or replaced without service interruption of unrelated traffic flows. In dual-Supervisor configurations, Cisco's Fast-Switchover will transfer switch control to the redundant Supervisor within seconds for mission-critical applications requiring maximum network availability. All system elements are also field replaceable units (FRUs) for maximizing serviceability and minimizing network downtime

For network-level resilience, Catalyst 6000 Family switches also support automatic recovery from failure using Spanning Tree per VLAN, and support load-sharing for faster link convergence using Fast EtherChannel or Gigabit EtherChannel technologies. Load balancing with even higher availability can also be accommodated using Cisco's MultiModule Channeling, where ports from different line cards can be aggregated into higher-bandwidth links. Catalyst 6000 Family switches are also capable of load balancing across Layer-3 paths.

For maximum availability, the Catalyst 6000 Family switches support Hot Standby Routing Protocol (HSRP), providing fast cutover to a backup system in the event of a catastrophic failure.

- Supervisor Engine supports hardware-based, wire-rate switching
  - —Scalable support for multiprotocol routing
  - —Address table for up to 32,000 MAC addresses

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0656
Doc. 3690

15.209

— Wire-rate learning

— Support for protocol filtering

- Support for both AC and DC power-supply options; also supports dual power-supply configurations
- Rack-mount hardware and cable guide available
- Console/Auxiliary port via RJ-45 (female) data terminal equipment (DTE) for local or remote connectivity

FlexWAN module

The FlexWAN module (WS-X6182-2PA) extends scalable WAN and MAN connectivity options to the Catalyst 6000 Family, simplifying network design and reducing the cost of network management, maintenance, and training. The FlexWAN module supports the majority of Cisco 7200 and 7500 WAN single wide interfaces, ranging from fractional T1/E1 to OC3 offering flexible migration options for Cisco 7200 and 7500 series customers and providing a bridge between existing LAN/WAN/MAN and legacy networks to future high-speed converged networks.

For more information on FlexWAN modules for the Catalyst 6000 Series, see

Content Switching Module (CSM)

The Cisco Content Switching Module (CSM) is a Catalyst 6500 line card that balances client traffic to farms of servers, firewalls, SSL devices, or VPN termination devices. The CSM provides a high-performance, cost-effective load balancing solution for enterprise and Internet Service Provider (ISP) networks. The CSM meets the demands of high-speed Content Delivery Networks, tracking network sessions and server load conditions in real time and directing each session to the most appropriate server. Fault tolerant CSM configurations maintain full state information and provide true hitless failover required for mission-critical functions.

For more information on Content Switching Module (CSM) modules for the Catalyst 6500 Series, see

Specifications

Hardware

Table 21-80: Technical Specifications for Catalyst 6000 Series and 6500 Series

Description	Specification
Switching Backplane	Catalyst 6000 Series: 32 Gbps Catalyst 6500 Series: Scalable to 256 Gbps
Memory	64 MB DRAM (Supervisor 1) 64 MB DRAM (MSFC); expandable to 128 MB 128 MB DRAM (MSFC2); expandable to 256 MB or 512 MB Optional 16 and 24 MB Flash PCMCIA cards
Interfaces	10 Gigabit Ethernet (LR, EX4 via SC) Gigabit Ethernet (SX LX/LH, and ZX interfaces via GBICs, MT-RJ, RJ-45) 100BaseFX MMF or SMF (MT-RJ) 10/100BaseTX (RJ-45 and RJ-21 Options) ATM OC12 (Single mode and Multimode Opt
Services Modules	Network Analysis Module Intrusion Detection Module Content Switching Module
Switch Load indicator	Approximates switch load from 1 to 100%

RQS nº 03/2005 - CN
CPMI - CORREIOS
0697
Fls. Nº
3690
Doc.

Description	Specification
Supervisor Engine Status LED	• Orange: Module is booting; Running diagnostics; Minor temperature threshold exceeded; • Green: All diagnostics pass; Module is operational • Red: Failed diagnostics; Major temperature threshold exceeded; Module not operational
System LED displays chassis environmental status	• Green: All chassis environmental monitors okay • Orange: Power supply failure; Incompatible power supplies installed; Power supply fan failure; Minor backplane temperature threshold exceeded; Redundant backplane clock failure • Red: Supervisor Engine over temperature condition; Major backplane temperature threshold exceeded
Supervisor Active LED	• Green: Operational and active • Orange: Standby mode
PWR MGMT (Power Management) LED	• Green: Sufficient power for all modules • Orange: Insufficient power for all modules
PCMCIA LED	Lights when the PCMCIA device is accessed
LINK LEDs for Gigabit Ethernet ports on the Supervisor Engine	• Green: Port is operational • Orange: Software disabled (solid); Disabled due to hardware failure (flashing)
Standard Network Protocols	IEEE 802.1Q, 802.1p, 802.3x Ethernet: IEEE 802.3, 10BaseT, and 10BaseFL Fast Ethernet: IEEE 802.3u, 100BaseTX, 10BaseFX Gigabit Ethernet: IEEE 802.3z

Table 21-81: Power Requirements for Catalyst 6000 Series and 6500 Series

Description	Specification
AC Input Current	1000 WAC: 13.2A max. @ 100 VAC 1000 WAC: 6.6A max. @ 200 VAC 1300 WAC: 17.6A max. @ 100 VAC 1300 WAC: 8.8A max. @ 200 VAC 2500 WAC: 17.6A max. @ 200 VAC (2500W output) 2500 WAC: 17.6A max. @ 100 VAC (1300W output) 4000 WAC: 26.4A max @ 200 VAC 4000 WAC: 24.0A max @ 220 VAC 4000 WAC: 21.8A max @ 240 VAC
DC Input current	1300 WDC: 38A @ 48 VDC 1300 WDC: 30A @ 60 VDC 2500 WDC: 70A @ 48 VDC 2500 WDC: 55A @ 60 VDC

15.208 A-
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0658
3690
Doc.

Description	Specification
KVA rating	1.8KVA for 1300W 3.6KVA for 2500W
AC Output power	1300W max. (low line operation: 100 - 120 VAC input) 2500W max. (high line operation: 200 - 240 VAC input)
DC Output power	1360W 2500W
Heat Dissipation	4300 BTU/hr max. for 1000 WAC 6140 BTU/hr max. for 1300 WAC 12000 BTU/hr max. for 2500 WAC/ 2500 WDC 18000 BTU/hr max. for 4000 WAC 6500 BTU/hr max. for 1300 WDC 1200 BTU/hr max. for 2500 WDC

Table 21-82: Physical and Environmental Specifications for Catalyst 6000 Series and 6500 Series

Description	Specification
Dimensions (H x W x D)	Catalyst 6006 and 6506 chassis: 20.1 x 17.2 x 18.1 in. (49.7 x 42.5 x 44.7 cm) Catalyst 6009 and 6509 chassis: 25.2 x 17.2 x 18.1 in. (62.3 x 42.5 x 44.7 cm) Catalyst 6509 vertical slot chassis: 33.5 x 17.2 x 18.1 in. (82.8 x 42.5 x 44.7 cm) Catalyst 6513 chassis: 33.3 x 17.2 x 18.1 in. (82.3 x 42.5 x 44.7 cm)
Minimum weight	65 lb (29.4 kg)
Maximum weight	242 lb (110 kg)
Mounting	19 in. (48.26 cm) rack-compatible (rack and cable guide hardware included)
Operating temperature	32 to 104°F (0 to 40°C)
Storage	-60 to 4000 m
Mean time between temperature	-40 to 167°F (-40 to 75°C)
Relative humidity	10 to 90%, noncondensing
Operating altitude failures (MTBF)	Seven years for system configuration

Table 21-83: Regulatory Approvals for Catalyst 6000 Series and 6500 Series

Description	Specification
Safety Certifications	UL 1950 EN 60950 CSA-C22.2 no. 950 IEC 60950 AS/NZA 3260 21 CFR 1040 EN 60825-1 IEC 60825-1TS 001

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0659
Doc. 3690

Description	Specification
Electromagnetic Emissions Certifications	FCC (CFR 47, Part 15) Class A VCCI CE Marking EN 55022 EN 55024 CISPR 22 AS/NZS 3548 NEBS Level 3 (GR-1089-CORE, GR-63-CORE) ETSI ETS-300386-2

Software

Table 21-84: Software Specifications for Catalyst 6000 Family

Description	Specification
Embedded Manageability	• NewFlow data export • TopN ports report • RMON agent • HC RMON (High Capacity, 64-bit counters) • Switched Port Analyzer (SPAN) and Enhanced-SPAN • Multiple Concurrent SPAN • Remote SPAN • Filtered SPAN • Syslog support • Telnet/command line interface support • IP TraceRoute • Domain Name Server (DNS) services • Network Time Protocol (NTP) • Cisco Discovery Protocol (CDP) v2 • VLAN Trunking Protocol (VTP) • IEEE Generic Attribute Registration Protocol (GARP) • IEEE GARP VLAN Registration Protocol (GVRP) • VLAN Query Protocol (VQP) • Simple Network Management Protocol (SNMP) v1, v2c, v3 • SNMP MIB-II support • SNMP MIB Additions and Enhancements Cisco-Switch-Engine-MIB Cisco-Memory-Pool-MIB Entity-MIB TraceRoute MIB • SNMP Traps • Multiple module software download • Multiple Default IP Gateway • Login banner for console

RQS nº 03/2005 - CN
CPMI - CORREIOS
0660
Fls. Nº
3690
Doc.

Description	Specification
Scalability	• IP Multilayer Switching • IP Multicast Multilayer Switching • IPX Multilayer Switching • Multi-protocol routing: Appletalk, DECnet, Vines, OSI, and CLNS • IP Routing Protocols: RIPv1/v2, OSPF, IGRP, EIGRP, BGP4, IS-IS • Jumbo Gigabit Ethernet Frame switching • Accelerated Server Load Balancing • IEEE GARP Multicast Registration Protocol • Fast EtherChannel/Gigabit EtherChannel/PAgP • ISL Trunking • 802.1Q / 802.1p • Dynamic Trunking Protocol (DTP) • Dynamic VLAN VMPS client • VTP, VTP version 2 • VTP Pruning
Bandwidth Management	• Protocol Filtering • Internet Group Management Protocol (IGMP) snooping • Broadcast suppression • Link load balancing • Fast EtherChannel (FEC) / Gigabit EtherChannel (GEC)
Network Resilience	• Redundant supervisors with Active Uplinks • BackboneFast convergence • UplinkFast convergence • PortFast convergence • FEC/GEC IP address-based Load Balancing • FEC/GEC Across Line Modules • Uni-Directional Link Detection (UDLD) • Interswitch Link (ISL) 802.1Q • Spanning Tree Protocol (STP) • Spanning Tree per VLAN • Enable/disable STP per VLAN • Hot Standby Router Protocol (HSRP) • Open Shortest Path First (OSPF) • Enhanced Internet Gateway Routing Protocol (EIGRP) • EtherChannel to Servers
Security Services	• Port Security • TACACS+ authentication • RADIUS Authentication • IP Permit list • Traps and syslog messages sent upon security violations • Advanced Layer 2/3/4 Intra-VLAN Access Lists (VACL) • Advanced Layer 3/4 Inter-VLAN Standard and Extended Access List • Reflexive ACL • Dynamic ACL • Policy-based Routing • Network Address Translation

RQS nº 03/2005 - CN
CPMI - CORREIOS
0661
Fls. Nº
3690
Doc.

Description	Specification
Quality of Service	• IP precedence detection and classification • 802.1Q/802.1p detection and classification • IP Differentiated Services packet detection and classification • Bandwidth Policing • Congestion Avoidance (Per-port WRED drop thresholds) • Traffic Scheduling (Per-port Weighted Round Robin queue scheduling) • COPS/RSVP • Port level delay and drop threshold settings
Multicast	• Cisco Group Management Protocol (CGMP) • Protocol Independent Multicast (PIM) (sparse and dense modes) • IGMP/IGMP snooping • IEEE GARP Multicast Registration Protocol (GMRP)

All software part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at http://www.cisco.com/cgi-bin/front.x/pricing

The Cisco Pricing Tool requires a user name and password. If you are not already registered, go to http://www.cisco.com/register and follow the instructions. After you have registered, you may access the Pricing Tool.

Ordering Information

Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at http://www.cisco.com/cgi-bin/front.x/pricing

The Cisco Pricing Tool requires a user name and password. If you are not already registered, go to http://www.cisco.com/register and follow the instructions. After you have registered, you may access the Pricing Tool.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0662
Doc. 3690

15.203
A.

Switch Tipo 1 doc 6

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0663
Doc. 3690

CHAPTER 11

Configuring EtherChannels

This chapter describes how to configure EtherChannels on the Catalyst 6000 family switch Layer 2 or Layer 3 LAN ports.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6000 Family IOS Command Reference* publication.

This chapter consists of these sections:

- Understanding How EtherChannels Work, page 11-1
- EtherChannel Feature Configuration Guidelines and Restrictions, page 11-5
- Configuring EtherChannels, page 11-6

Note The commands in the following sections can be used on all LAN ports in Catalyst 6000 family switches, including the ports on the supervisor engine and a redundant supervisor engine.

Understanding How EtherChannels Work

These sections describe how EtherChannels work:

- EtherChannel Feature Overview, page 11-1
- Understanding How EtherChannels Are Configured, page 11-2
- Understanding Port Channel Interfaces, page 11-4
- Understanding Load Balancing, page 11-5

EtherChannel Feature Overview

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.

A Catalyst 6000 family switch supports a maximum of 64 EtherChannels (256 with Release 12.0(5)WX(2)E and earlier). You can form an EtherChannel with up to eight compatibly configured Ethernet ports on any module in a Catalyst 6000 family switch. All LAN ports in each EtherChannel must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports.

15.202 A
Rubrica
Fls. Nº 0664
Doc. 3690

15.203 A-

Note The network device to which a Catalyst 6000 family switch is connected may impose its own limits on the number of ports in an EtherChannel.

If a segment within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining segments within the EtherChannel. When a failure occurs, the EtherChannel feature sends a trap that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one segment in an EtherChannel are blocked from returning on any other segment of the EtherChannel.

Understanding How EtherChannels Are Configured

These sections describe how EtherChannels are configured:

- EtherChannel Configuration Overview, page 11-2
- Understanding Manual EtherChannel Configuration, page 11-3
- Understanding PAgP EtherChannel Configuration, page 11-3
- Understanding IEEE 802.3ad LACP EtherChannel Configuration, page 11-3

EtherChannel Configuration Overview

You can configure EtherChannels manually or you can use the Port Aggregation Control Protocol (PAgP) or, with Release 12.1(11b)EX and later, the Link Aggregation Control Protocol (LACP) to form EtherChannels. The EtherChannel protocols allow ports with similar characteristics to form an EtherChannel through dynamic negotiation with connected network devices. PAgP is a Cisco-proprietary protocol and LACP is defined in IEEE 802.3ad.

PAgP and LACP do not interoperate with each other. Ports configured to use PAgP cannot form EtherChannels with ports configured to use LACP. Ports configured to use LACP cannot form EtherChannels with ports configured to use PAgP.

Table 11-1 lists the user-configurable EtherChannel modes.

Table 11-1 EtherChannel Modes

Mode	Description
on	Mode that forces the LAN port to channel unconditionally. In the **on** mode, a usable EtherChannel exists only when a LAN port group in the **on** mode is connected to another LAN port group in the **on** mode. Because ports configured in the **on** mode do not negotiate, there is no negotiation traffic between the ports.
auto	PAgP mode that places a LAN port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP negotiation. (Default)
desirable	PAgP mode that places a LAN port into an active negotiating state, in which the port initiates negotiations with other LAN ports by sending PAgP packets.
passive	LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. (Default)
active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0665
Fls. Nº
3690
Doc.
78-14394-01

15.200
JA.

Understanding Manual EtherChannel Configuration

Manually configured EtherChannel ports do not exchange EtherChannel protocol packets. A manually configured EtherChannel forms only when you enter configure all ports in the EtherChannel compatibly.

Understanding PAgP EtherChannel Configuration

PAgP supports the automatic creation of EtherChannels by exchanging PAgP packets between LAN ports. PAgP packets are exchanged only between ports in **auto** and **desirable** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once PAgP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **auto** and **desirable** modes allow PAgP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different PAgP modes if the modes are compatible. For example:

- A LAN port in **desirable** mode can form an EtherChannel successfully with another LAN port that is in **desirable** mode.
- A LAN port in **desirable** mode can form an EtherChannel with another LAN port in **auto** mode.
- A LAN port in **auto** mode cannot form an EtherChannel with another LAN port that is also in **auto** mode, because neither port will initiate negotiation.

Understanding IEEE 802.3ad LACP EtherChannel Configuration

LACP supports the automatic creation of EtherChannels by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in **passive** and **active** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **passive** and **active** modes allow LACP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A LAN port in **active** mode can form an EtherChannel successfully with another LAN port that is in **active** mode.
- A LAN port in **active** mode can form an EtherChannel with another LAN port in **passive** mode.
- A LAN port in **passive** mode cannot form an EtherChannel with another LAN port that is also in **passive** mode, because neither port will initiate negotiation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0666
Doc. 3690

15.1.99
A.

LACP uses the following parameters:

- LACP system priority—You must configure an LACP system priority on each switch running LACP. The system priority can be configured automatically or through the CLI (see the "Configuring the LACP System Priority and System ID" section on page 11-9). LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other systems.

Note The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

- LACP port priority—You must configure an LACP port priority on each port configured to use LACP. The port priority can be configured automatically or through the CLI (see the "Configuring Channel Groups" section on page 11-7). LACP uses the port priority with the port number to form the port identifier. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
- LACP administrative key—LACP automatically configures an administrative key value equal to the channel group identification number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:
  - Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
  - Configuration restrictions that you establish

On ports configured to use LACP, LACP tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware (eight ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails. You can configure an additional 8 standby ports (total of 16 ports associated with the EtherChannel).

Understanding Port Channel Interfaces

Each EtherChannel has a numbered port channel interface. Release 12.1(5)E and later supports a maximum of 64 port channel interfaces, numbered from 1 to 256.

Note Releases 12.1(4)E1, 12.1(3a)E4, and 12.1(3a)E3 support a maximum of 64 port channel interfaces, numbered from 1 to 64. Releases 12.1(2)E and earlier support a maximum of 256 port channel interfaces, numbered from 1 to 256.

The configuration that you apply to the port channel interface affects all LAN ports assigned to the port channel interface.

After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel; the configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port channel interface, for example, Spanning Tree Protocol (STP) commands or commands to configure a Layer 2 EtherChannel as a trunk.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0667
Fls. Nº
3690
Doc.

15.198
-A-

Understanding Load Balancing

An EtherChannel balances the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses or IP addresses. With a PFC2, EtherChannel load balancing can also use Layer 4 port numbers. EtherChannel load balancing can use either source or destination or both source and destination addresses or ports. The selected mode applies to all EtherChannels configured on the switch.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel; using source addresses or IP addresses might result in better load balancing.

EtherChannel Feature Configuration Guidelines and Restrictions

When EtherChannel interfaces are configured improperly, they are disabled automatically to avoid network loops and other problems. To avoid configuration problems, observe these guidelines and restrictions:

- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannels (maximum of eight LAN ports) with no requirement that the LAN ports be physically contiguous or on the same module.
- Configure all LAN ports in an EtherChannel to use the same EtherChannel protocol; you cannot run two EtherChannel protocols in one EtherChannel.
- Configure all LAN ports in an EtherChannel to operate at the same speed and in the same duplex mode.
- LACP does not support half-duplex. Half-duplex ports in an LACP EtherChannel are put in the suspended state.
- Enable all LAN ports in an EtherChannel. If you shut down a LAN port in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining ports in the EtherChannel.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.
- For Layer 3 EtherChannels, assign Layer 3 addresses to the port channel logical interface, not to the LAN ports in the channel.
- For Layer 2 EtherChannels:
  - Assign all LAN ports in the EtherChannel to the same VLAN or configure them as trunks.
  - If you configure an EtherChannel from trunking LAN ports, verify that the trunking mode is the same on all the trunks. LAN ports in an EtherChannel with different trunk modes can operate unpredictably.
  - An EtherChannel supports the same allowed range of VLANs on all the LAN ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the LAN ports do not form an EtherChannel.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0668
Doc. 3690

15.191

  - LAN ports with different STP port path costs can form an EtherChannel as long they are compatibly configured with each other. If you set different STP port path costs, the LAN ports are not incompatible for the formation of an EtherChannel.
  - An EtherChannel will not form if protocol filtering is set differently on the LAN ports.
- After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel. The configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration.

Configuring EtherChannels

These sections describe how to configure EtherChannels:

- Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels, page 11-6
- Configuring Channel Groups, page 11-7
- Configuring EtherChannel Load Balancing, page 11-10

Note Make sure that the LAN ports are configured correctly (see the "EtherChannel Feature Configuration Guidelines and Restrictions" section on page 11-5).

Note With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode commands by entering the **do keyword before the** EXEC mode command.

Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels

When configuring port channel logical interfaces for Layer 3 EtherChannels, note the following:

- When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port channel logical interfaces. If you are configuring a Layer 2 EtherChannel, do not perform the procedures in this section (see the "Configuring Channel Groups" section on page 11-7).
- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface as described in this section, and then put the Layer 3 LAN ports into the channel group (see the "Configuring Channel Groups" section on page 11-7).
- To move an IP address from a Layer 3 LAN port to an EtherChannel, you must delete the IP address from the Layer 3 LAN port before configuring it on the port channel logical interface.

To create a port channel interface for a Layer 3 EtherChannel, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface port-channel number`	Creates the port channel interface.
	`Router(config)# no interface port-channel number`	Deletes the port channel interface.
Step 2	`Router(config-if)# ip address ip_address mask`	Assigns an IP address and subnet mask to the EtherChannel.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0669
3690
Doc.

15.196
A.

	Command	Purpose
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show running-config interface port-channel` *number*	Verifies the configuration.

When creating the port channel interface, the *group* number can be one of the following:

- Release 12.1(5)E and later—1 through 256, up to a maximum of 64 port channel interfaces
- Releases 12.1(4)E1, 12.1(3a)E4, and 12.1(3a)E3—1 through 64
- Release 12.1(2)E and earlier—1 through 256

This example shows how to create port channel interface 1:

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# ip address 172.32.52.10 255.255.255.0
Router(config-if)# end
```

This example shows how to verify the configuration of port channel interface 1:

```
Router# show running-config interface port-channel 1
Building configuration...

Current configuration:
!
interface Port-channel1
 ip address 172.32.52.10 255.255.255.0
 no ip directed-broadcast
end
Router#
```

Configuring Channel Groups

When configuring channel groups, note the following:

- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface first (see the "Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels" section on page 11-6), and then put the Layer 3 LAN ports into the channel group as described in this section.
- When configuring Layer 2 EtherChannels, configure the LAN ports with the **channel-group** command as described in this section, which automatically creates the port channel logical interface. You cannot put Layer 2 LAN ports into a manually created port channel interface.
- For Cisco IOS to create port channel interfaces for Layer 2 EtherChannels, the Layer 2 LAN ports must be connected and functioning.

To configure channel groups, perform this task for each LAN port:

	Command	Purpose
Step 1	`Router(config)# interface` *type*[1] *slot/port*	Selects a LAN port to configure.
Step 2	`Router(config-if)# no ip address`	Ensures that there is no IP address assigned to the LAN port.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0670
Fls. Nº
3690
Doc.

15.195
JA

	Command	Purpose
Step 3	`Router(config-if)# channel-protocol {lacp | pagp}`	(Optional) On the selected LAN port, restricts the **channel-group** command to the EtherChannel protocol configured with the **channel-protocol** command.
	`Router(config-if)# no channel-protocol`	Removes the restriction.
Step 4	`Router(config-if)# channel-group` *number* `mode {active | auto | desirable | on | passive}`	Configures the LAN port in a port channel and specifies the mode (see Table 11-1 on page 11-2).
	`Router(config-if)# no channel-group`	Removes the LAN port from the channel group.
Step 5	`Router(config-if)# lacp port-priority` *priority_value*	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	`Router(config-if)# no lacp port-priority`	Reverts to the default.
Step 6	`Router(config-if)# end`	Exits configuration mode.
Step 7	`Router# show running-config interface` *type*[1] *slot/port* `Router# show interfaces` *type*[1] *slot/port* `etherchannel`	Verifies the configuration.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure Fast Ethernet ports 5/6 and 5/7 into port channel 2 with PAgP mode **desirable**:

```
Router# configure terminal
Router(config)# interface range fastethernet 5/6 -7
Router(config-if)# channel-group 2 mode desirable
Router(config-if)# end
```

Note See the "Configuring a Range of Interfaces" section on page 5-4 for information about the **range** keyword.

This example shows how to verify the configuration of port channel interface 2:

```
Router# show running-config interface port-channel 2
Building configuration...

Current configuration:
!
interface Port-channel2
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 5/6:

```
Router# show running-config interface fastethernet 5/6
Building configuration...

Current configuration:
!
interface FastEthernet5/6
 no ip address
 switchport
```

RQS nº 03/2005 - CN
CPMI CORREIOS
0611
Fls. Nº
3690
Doc.

15.194 A-

```
 switchport access vlan 10
 switchport mode access
 channel-group 2 mode desirable
end
Router# show interfaces fastethernet 5/6 etherchannel
Port state    = Down Not-in-Bndl
Channel group = 12          Mode = Desirable-Sl     Gcchange = 0
Port-channel  = null        GC   = 0x00000000          Pseudo port-channel = Po1
2
Port index    = 0           Load = 0x00        Protocol =   PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                                 Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers   Interval Count    Priority   Method  Ifindex
Fa5/2     d     U1/S1              1s       0         128        Any      0

Age of the port in the current state: 04d:18h:57m:19s
```

This example shows how to verify the configuration of port channel interface 2 after the LAN ports have been configured:

```
Router# show etherchannel 12 port-channel
                Port-channels in the group:
                ----------------------

Port-channel: Po12
------------

Age of the Port-channel   = 04d:18h:58m:50s
Logical slot/port   = 14/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   PAgP

Router#
```

Configuring the LACP System Priority and System ID

The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

To configure the LACP system priority and system ID, perform this task:

	Command	Purpose
Step 1	`Router(config)# lacp system-priority` *priority_value*	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	`Router(config)# no system port-priority`	Reverts to the default.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show lacp sys-id`	Verifies the configuration.

RDS - 03/2005 - CN
SEM - CORREIOS
0672
Fls: Nº
3690
Doc.

15.193 (A)

This example shows how to configure the LACP system priority:

```
Router# configure terminal
Router(config)# lacp system-priority 23456
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show lacp sys-id
23456,0050.3e8d.6400
Router#
```

The system priority is displayed first, followed by the MAC address of the switch.

Configuring EtherChannel Load Balancing

To configure EtherChannel load balancing, perform this task:

	Command	Purpose
Step 1	`Router(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port}`	Configures EtherChannel load balancing.
	`Router(config)# no port-channel load-balance`	Reverts to default EtherChannel load balancing.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show etherchannel load-balance`	Verifies the configuration.

The load-balancing keywords indicate the following information:

- With a PFC2:
  - **src-port**—Source Layer 4 port
  - **dst-port**—Destination Layer 4 port
  - **src-dst-port**—Source and destination Layer 4 port
- With a PFC or PFC2:
  - **src-ip**—Source IP addresses
  - **dst-ip**—Destination IP addresses
  - **src-dst-ip**—Source and destination IP addresses
  - **src-mac**—Source MAC addresses
  - **dst-mac**—Destination MAC addresses
  - **src-dst-mac**—Source and destination MAC addresses

This example shows how to configure EtherChannel to use source and destination IP addresses:

```
Router# configure terminal
Router(config)# port-channel load-balance src-dst-ip
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show etherchannel load-balance
Source XOR Destination IP address
Router#
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
0673
Fls. Nº
3690
Doc.

15.192
A.

Switch Tipo 1 doc 7

RQS nº 03/2005 - CN
CPMI CORREIOS
0674
Fls. Nº
3690
Doc.

15.191
A-

Technical Specifications

This appendix provides the technical specifications for the Catalyst 6000 family switches:

- Catalyst 6006 and 6506 Switches, page A-2
- Catalyst 6009 and 6509 Switches, page A-4
- Catalyst 6509-NEB Switch, page A-5
- Catalyst 6513 Switch, page A-7
- Catalyst 6000 Family Power Supplies, page A-8
- Regulatory Standards Compliance, page A-10

Refer to the *Catalyst 6000 Family Module Installation Guide* for module and interface port specifications.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0675
Doc. 3690

15.190
A.

Catalyst 6006 and 6506 Switches

The Catalyst 6006 and Catalyst 6506 switch specifications are provided in Table A-1.

Table A-1 Catalyst 6006 Switch/Catalyst 6506 Switch Specifications

Item	Specification
Environmental	
Temperature, ambient operating	32°F (0°C) to 104°F (40°C)
Temperature, ambient nonoperating and storage	–40°F (–40°C) to 158°F (70°C)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Humidity (RH), ambient (noncondensing) nonoperating and storage	5% to 95%
Altitude, operating	Sea level to 6500 feet (2000 m)
Noise levels	45.8 to 49.6 dBa
Physical Characteristics	
Dimensions (H x W x D)	20.1 x 17.25 x 18.4 in. (51.1 x 43.1 x 46.0 cm) Chassis depth including cable guide is 21.64 in. (55.0 cm). Chassis requires 12 RU.
Weight	Chassis only: 45 lb (20.41 kg)
	Chassis fully configured with 1 supervisor engine, 5 switching modules, and 2 power supplies: 115 lb (52.15 kg)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0676
Doc. 3690

15.189
A-

Table A-1 Catalyst 6006 Switch/Catalyst 6506 Switch Specifications (continued)

Item	Specification
Power Supply	1000W AC-input, 1300W AC-input or DC-input, 2500W AC-input or 2500W DC-input power supplies. An optional second power supply can be installed in the chassis.
Airflow	200 lfm[1] through system fan assembly. We recommend that you maintain a minimum air space of 6 inches (16 cm) between walls and the chassis air vents and a minimum separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

1. lfm = linear feet per minute

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0677
Doc 3690

15.188
A-

Catalyst 6009 and 6509 Switches

The Catalyst 6009 and Catalyst 6509 switch specifications are provided in Table A-2.

Table A-2 Catalyst 6009 Switch/Catalyst 6509 Switch Specifications

Item	Specification
Environmental	
Temperature, ambient operating	32°F (0°C) to 104°F (40°C)
Temperature, ambient nonoperating and storage	–40°F (–40°C) to 158°F (70°C)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Humidity (RH), ambient (noncondensing) nonoperating and storage	5% to 95%
Altitude, operating	Sea level to 6500 feet (2000 m)
Noise levels	49.8 to 53.6 dBa
Physical Characteristics	
Dimensions (H x W x D)	25.5 x 17.25 x 18.4 in. (64.8 x 43.1 x 46.0 cm) Chassis depth including cable guide is 21.64 in. (55.0 cm). Chassis requires 15 RU.
Weight	Chassis only: 55 lb (24.9 kg)
	Chassis fully configured with 1 supervisor engine, 8 switching modules, and 2 power supplies: 135 lb (61.2 kg)

RQS nº 03/2005 - CN
CPMI - CORREIOS
0678
Fls. Nº
3690
Doc:

Table A-2 Catalyst 6009 Switch/Catalyst 6509 Switch Specifications (continued)

Item	Specification
Power Supply	1300W AC-input or DC-input, 2500W AC-input or DC-input power supply, or 4000W AC-input power supply. An optional second power supply can be installed in the chassis.
Airflow	200 lfm[1] through system fan assembly. We recommend that you maintain a minimum air space of 6 inches (16 cm) between walls and the chassis air vents and a minimum separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

1. lfm = linear feet per minute

Catalyst 6509-NEB Switch

The Catalyst 6509-NEB switch specifications are provided in Table A-3.

Table A-3 Catalyst 6509-NEB Switch Specifications

Item	Specification
Environmental	
Temperature, ambient operating	32°F (0°C) to 104°F (40°C)
Temperature, ambient nonoperating and storage	–40°F (–40°C) to 158°F (70°C)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Humidity (RH), ambient (noncondensing) nonoperating and storage	5% to 95%
Altitude, operating	Sea level to 6500 feet (2000 m)
Noise levels	54.2 to 56.4 dBa

RQS nº [redacted] - CN
CPMI - CORREIOS
Fls. Nº 0679
Doc. 3690

15.186
A-

Table A-3 Catalyst 6509-NEB Switch Specifications (continued)

Item	Specification
Physical Characteristics	
Dimensions (H x W x D)	33.5 x 17.25 x 18.1 inches (85.1 x 43.1 x 46 cm). Chassis requires 20 RU.
Weight	Chassis only: 55 lb (24.9 kg) Chassis fully configured with 1 supervisor engine, 8 switching modules, and 2 power supplies: 135 lb (61.2 kg)
Power Supply	1300W AC-input or DC-input, 2500W AC-input or DC-input, or 4000W AC-input power supply. An optional second power supply can be installed in the chassis.
Airflow	200 lfm[1] through system fan assembly. We recommend that you maintain a minimum air space of 6 inches (16 cm) between walls and the chassis air vents and a minimum 12 inches (30.5 cm) separation between two chassis to prevent overheating.

1. lfm = linear feet per minute

ROS nº 03/2005 - CN
CPMI - CORREIOS
78-5050-11
Fls. Nº 0680
Doc. 3690

15.185
A.

Catalyst 6513 Switch

The Catalyst 6513 switch specifications are provided in Table A-4.

Table A-4 Catalyst 6513 Switch Specifications

Item	Specification
Environmental	
Temperature, ambient operating	32°F (0°C) to 104°F (40°C)
Temperature, ambient nonoperating and storage	–40°F (–40°C) to 158°F (70°C)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Humidity (RH), ambient (noncondensing) nonoperating and storage	5% to 95%
Altitude, operating	Sea level to 6500 feet (2000 m)
Noise levels	58.1 to 61.4 dBa
Physical Characteristics	
Dimensions (H x W x D)	33.15 x 17.3 x 18.1 inches (84.2 x 43.9 x 46 cm). Chassis requires 19 RU.
Weight	Chassis fully configured with 2 supervisor engines, 11 switching modules, and 2 power supplies: 240 lb (108.9 kg)
Power Supply	2500W AC- or DC-input or 4000W AC-input power supply. An optional second power supply can be installed in the chassis.
Airflow	250 lfm[1] through system fan assembly. We recommend that you maintain a minimum air space of 6 inches (16 cm) between walls and the chassis air vents and a minimum separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

1. lfm = linear feet per minute

ROS nº 03/2005 - CN
CP A-7 RREIOS
Fls. Nº 0681
Doc. 3690

15.134
A.

Catalyst 6000 Family Power Supplies

Table A-5 lists the specifications for the Catalyst 6000 family power supplies.

Table A-5 Catalyst 6000 Power Supply Specifications

Item	Specification
1000W AC-input Power Supply	
AC-input type	Autoranging input with power factor corrector.
AC-input voltage	100 to 240 VAC (10% for full range).
AC-input current	12A @ 100 VAC, 6A @ 240 VAC.
AC-input frequency	50/60 Hz (nominal) (3 Hz for full range).
Power supply output capacity	1000W.
Power supply output	15A @ +3.3V, 5A @ +5V, 6A @ +12V, 20.3A @ +42V.
Output holdup time	20 ms minimum.
1300W AC- and DC-input Power Supplies[1]	
AC-input type	Autoranging input with power factor corrector.
AC-input voltage	100 to 240 VAC (10% for full range).
AC-input current	17.25A @ 100 VAC, 8A @ 200 VAC.
AC-input frequency	50/60 Hz (nominal) (3 Hz for full range).
DC-input voltage	–48 VDC to –60 VDC continuous.
DC-input current	38A @ -48 VDC, 30A @ -60 VDC.
Power supply output capacity	1300W maximum AC-input; 1360W DC-input.
Power supply output (AC supply)	15A @ +3.3V, 5A @ +5V, 6A @ +12V, 27.46A @ +42V.
Power supply output (DC supply)	15A @ +3.3V, 5A @ +5V, 6A @ +12V, 30A @ +42V.
DC input terminal block	Accepts 3–10 AWG copper conductors. Actual size of the wire needed is determined by the installer or local electrician. Terminal block material rated at 120°C.
Output holdup time	20 ms minimum (AC-input power supply).
	8 ms (DC-input power supply).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0682
Doc 3690

15.183
A.

Table A-5 Catalyst 6000 Power Supply Specifications (continued)

Item	Specification
2500W AC- and DC-input Power Supplies	
AC-input type	Autoranging input with power factor corrector.
AC-input voltage	100 to 120 VAC, 200 to 240 VAC (10% for full range).
AC-input current	16A maximum at 200 VAC at 2500W output. 16A maximum at 100 VAC at 1300W output.
AC-input frequency	50/60 Hz (nominal) (3% for full range).
Power supply output capacity	1300W maximum (100–120 VAC). 2500W maximum (200–240 VAC or –48 to –60 VDC).
System power dissipation	3520W (total input power) or 3.6 KVA (high-line operation).
DC-input voltage	–48 VDC to –60 VDC continuous.
DC-input current	80A.
Power supply output (AC supply)	15.5A @ +3.3V, 5A @ +5V, 6A @ +12V, 27.5A @ +42V (100/120VAC). 15A @ +3.3V, 5A @ +5V, 10A @ +12V, 55.5A @ +42V (200/240VAC).
Power supply output (DC supply)	15A @ +3.3V, 5A @ +5V, 10A @ +12V, 55.5A @ +42V.
DC input terminal block	Accepts 2–14 AWG copper conductors. Actual size of the wire needed is determined by the installer or local electrician. Terminal block material rated at 150°C.
Output holdup time	20 ms minimum (AC-input power supply). 4 ms (DC-input power supply).

RQS-nº 03/2005 - CN
CPMI CORREIOS
0689
A-9
Fls. Nº
Doc 3690

15.182
A.

Table A-5 Catalyst 6000 Power Supply Specifications (continued)

Item	Specification
4000W AC-input Power Supply	
AC-input type	High-line input with power factor corrector, 30A single-phase circuit.
AC-input voltage	200 to 240 VAC (10% for full range).
AC-input current	23A.
Power supply output capacity	4000W maximum.
AC-input frequency	50/60 Hz (nominal) (3% for full range).
KVA rating	5.4 kVA maximum.
Maximum output current	15A @ +3.3V, 5A @ +5V, 10A @ +12V, 91.20A @ +42V.
Output holdup time	20 ms minimum.

1. Some early versions of the 1300W AC-input power supply were marked as 1800W. This value refers to the input power rating or maximum system power dissipation of the power supply. The output power of the power supply is 1300W. Power supplies currently shipping are marked as 1300W.

Regulatory Standards Compliance

Catalyst 6000 family switches comply with the regulatory standards listed in the *Regulatory Compliance and Safety Information for the Catalyst 6000 Family Switches* document.

RQS nº 03/2005 - CN
CPMI - CORREIOS
78/6050-11
Fls. Nº 0684
3690
Doc.

15.181
A.

Switch Tipo 1 doc 8

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0685
Doc. 3690

Cisco Systems

15.180
A-

Data Sheet

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 **Ethernet** Interface Modules

As Cisco's premier modular multilayer switch, the Catalyst® 6500 Series delivers secure, converged services from the wiring closet to the core, to the data center, to the WAN edge.

The Cisco Catalyst® 6500 Series provides the broadest selection of 10/100 and 10/100/1000 Ethernet media, inline power options, densities, performance, interoperability, and chassis deployments. Equally suited for basic wiring closets, small campus distribution/core layers, and high performance data centers, Catalyst 6500 10/100 and 10/100/1000Mbps modules scale from 16-ports up to 576-ports in a single Catalyst 6500 chassis. Catalyst 6500 10/100 and 10/100/1000Mbps modules feature:

- Proven and widely deployed Cisco AVVID wiring closet solution—Cisco's most widely deployed IP telephony port-enabled campus switch
- Choice of media and connector types—Available in copper unshielded twisted-pair (UTP), shielded twisted-pair (STP) using RJ-45 or RJ-21, multimode fiber (62.5/125 micron), and single-mode fiber using MT-RJ 100FX and 10FL
- IP phone and wireless access point support—Support inline power field upgrade (copper only), NIC/Phone auto-detection (phone discovery), and voice VLANs
- Simplified network operation with cable fault detection—Test cabling using Time Domain Reflectometer (TDR) that sends signals down the cable to identify faults in each twisted pair (available for 10/100/1000 copper
- Range of port densities—Available with 16 to 48 ports per module; enabling up to 576 10/100/1000Base-TX ports, 288 ports of 100-Base-FX, or 10BASE-FL per 13-slot chassis (configured with 12 interface modules)
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules) and 256 Gbps bandwidth/210 Mpps(dCEF256 interface modules)
- IEEE 802.3 triple-speed autonegotiation—Allow switches to negotiate speed (10, 100, and now 1000 Mbps) and duplex mode (half or full) with attached devices
- Superior traffic management—Available with large 1-MB-per-interface buffers and up to 8 transmit queues for traffic prioritization and policing

RQS nº 03/2005 - CN
CPMI - CORREIOS
0686
Fls. Nº
3690
Doc.

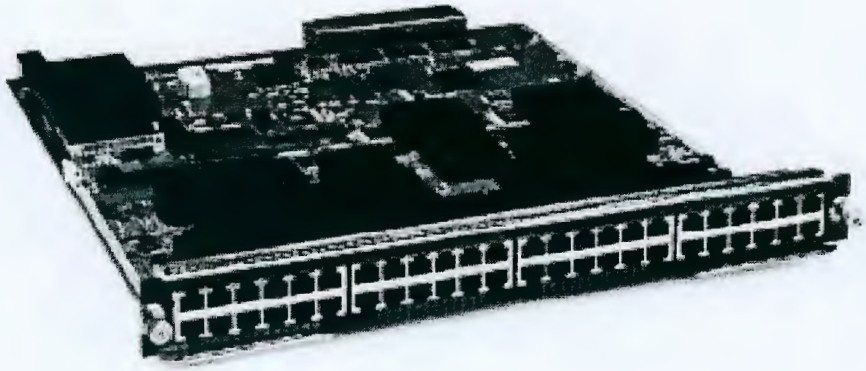
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-179
A-

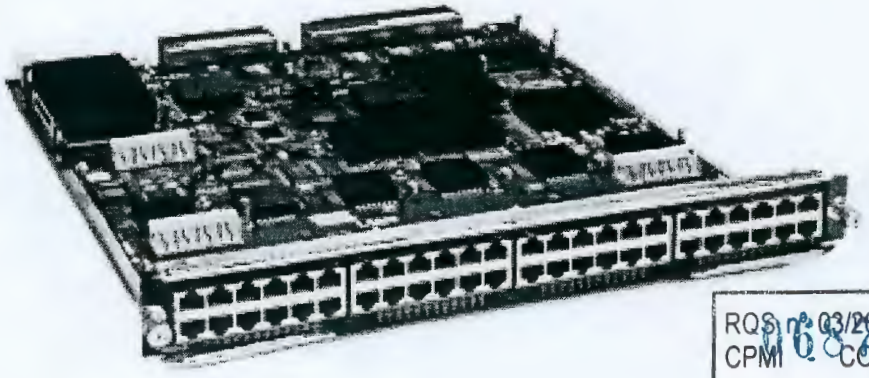
- Operational consistency—Supported in all Catalyst 6500 3-, 6-, 9-, and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software; interoperable with all other interfaces and services modules; and forward-compatible with all Catalyst 6500 supervisor engines
- Maximum network uptime and resiliency—Support Cisco enhanced Per-Virtual LAN (VLAN) Spanning Tree Plus (PVST+) protocol, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree (MST) protocol, Per-VLAN Rapid Spanning Tree (PVRST) protocol, Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Cisco EtherChannel®, and IEEE 802.3ad link aggregation for fault-tolerant connectivity
- Extensive management tools—Support CiscoWorks network management platform; Simple Network Management Protocol (SNMP) versions 1, 2, and 3; and four Remote Monitoring (RMON) groups (statistics, history, alarms, and events)

The newest members of the Cisco Catalyst 6500 Series 10/100/1000 product family—the Classic interface module WS-X6148-GE-TX and the CEF256 interface module WS-X6548-GE-TX—provide 10/100/1000 Gigabit Ethernet over copper network access using standard RJ-45 connectors (Figure 1).

Figure 1
Cisco Catalyst 6500 Series 48-Port RJ-45 10/100/1000 Ethernet Interface Modules
WS-X6148-GE-TX



WS-X6548-GE-TX



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1687
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.178
A-

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Applications

Ethernet and Fast Ethernet 10/100 and 10/100/1000 interface modules are used in both wiring closet and data center applications (Figure 2; Table 1).

Table 1 Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Copper Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connector/ Interface	Inline Power Support[1]	Queues per Port (Tx = Transmit, Rx = Receive)[2]	Buffer Size
Data Center and Server Farm	WS-X6516-GE-TX	CEF256	16, RJ-45, 10/100/1000	No	Tx–1p2q2T, Rx–1p1q4T	512 KB per port
Server Farm	WS-X6548-RJ-45	CEF256	48, RJ-45, 10/100	No	Tx–1p3q1t, Rx–1p1q0t	1 MB per port
Server Farm	WS-X6548-RJ-21	CEF256	48, RJ-21, 10/100	No	Tx–1p3q1t, Rx–1p1q0t	1 MB per port
Premier Wiring Closet	WS-X6548V-GE-TX	CEF256, No upgrade to dCEF	48, RJ-45, 10/100/1000	Both	Tx–1p2q2t (per 8 ports), Rx–1p2t (per port)	1 MB per 8 ports
Premier Wiring Closet	WS-X6548-GE-TX	CEF256, No upgrade to dCEF	48, RJ-45, 10/100/1000	Both, Upgr	Tx–1p3q1t, Rx–1p1q4t	1 MB per 8 ports
Wiring Closet	WS-X6148V-GE-TX	Classic	48, RJ-45, 10/100/1000	Both	Tx–1p2q2t, Rx–1q2t	1 MB per 8 ports
Wiring Closet	WS-X6148-GE-TX	Classic	48, RJ-45, 10/100/1000	Both, Upgr	Tx–1p2q2t, Rx–1q2t	1 MB per 8 ports
Base Wiring Closet	WS-X6148-RJ45V	Classic	48, RJ-45, 10/100/1000	Both	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ21V	Classic	48, RJ-21, 10/100	Both	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ-45	Classic	48, RJ-45, 10/100	Both, Upgr	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ-21	Classic	48, RJ-21, 10/100	Both, Upgr	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6348-RJ45V	Classic	48, RJ-45, 10/100	Cisco	Tx 2q2t, Rx 1q4t	128 KB per port
Base Wiring Closet	WS-X6348-RJ21V	Classic	48, RJ-21, 10/100	Cisco	Tx 2q2t, Rx 1q4t	128 KB per port

1. Inline Power Legend:
Both = Cisco inline power (available now) and IEEE 802.3af (via future field upgradable daughter card)
Cisco = Cisco inline power only
Upgr = shipped as data only but upgradable to the inline power type specified
No = inline power not supported

2. **Queues Legend:** 1p7q8t = 1 priority queue, 7 round robin queues, 8 thresholds

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0688
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.171
A.

Table 2 Cisco Catalyst 6500 Series 100FX and 10FL Fiber Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connectors/ Interface Media	Queues per Port (Tx = Transmit, Rx = Receive)[1]	Buffers
Access, Server Farm	WS-X6524-100FX-MM	CEF256, Upgradable to dCEF	24, MM MT-RJ, 100FX	Tx 1p3q1t, Rx 1p1q0t	1 MB per port
Access, Server Farm	WS-X6324-100FX-MM	Classic	24, MM, MT-RJ, 100FX	Tx 2q2t, Rx 1q4t	128 KB per port
Access, Server Farm	WS-X6324-100FX-SM	Classic	24, SM MT-RJ, 100FX	Tx 2q2t, Rx 1q4t	128 KB per port
Access	WS-X6024-10FL-MT	Classic	24, MM MT-RJ, 10FL	Tx 2q2t, Rx 1q4t	64 KB per port

1. **Queues Legend:** 1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0689
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.1-46
A.

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules with Cisco Inline Power

The Cisco Catalyst 6500 Series delivered the first 10/100BASE-T Ethernet switching modules that provided inline power for converged data and voice traffic as well as other inline powered devices, such as wireless access points. Several Catalyst 6500 series interface modules support inline power or "power over Ethernet" on each interface port, allowing customers to build campus multiservice data and voice networks for wiring closets with the following features:

- Inline power—Provides 48-volt DC power (for Cisco Inline Power and IEEE 802.3af standard inline power when it becomes available) over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters for IP phones and wireless access points
- Phone discovery—Detects the presence of an IP phone and supplies inline power automatically
- Auxiliary VLAN using 802.1Q—Segments IP phones and data endpoints into separate logical networks automatically
- AutoQoS—Simplifies the task of configuring QoS mechanisms for IP telephony and more

Cisco Catalyst Inline Power and IEEE 802.3af Inline Power

The Inline Power feature gives network administrators centralized power control. It works over existing Category 5 UTP installations and helps to ensure that building power outages will not affect network telephony connections, providing greater network availability—when Cisco Catalyst 6500 Series switches are configured with uninterruptible power supply (UPS) systems.

Several 10/100 and 10/100/1000 Ethernet interface modules support the Cisco Inline Power feature today, enabled by a daughter card for "pay as grow" flexibility. Once ratified, some of these interface modules will also support the IEEE 802.3af standard as an additional upgrade option. The Cisco Catalyst Inline Power feature implementation passes the required domestic and international safety regulations and compliance measures.

Phone Discovery

The Cisco phone discovery feature eases network management burdens by automating the Inline Power feature. With phone discovery, the Cisco Catalyst switch detects the presence of an IP phone and supplies inline power automatically, eliminating the need to manually enable ports for inline power. The phone discovery mechanism is intelligent enough to differentiate between an IP phone and a network interface card (NIC), and will not supply inline power to NICs or other devices not designed to use inline power. With this feature, network administrators can depend on automatic and centralized control of inline power that is safe to deploy and maintain.

Auxiliary VLAN

The unique Auxiliary VLAN feature offered by Cisco provides automatic VLAN configuration for IP phones. It places phones into their own VLANs automatically, simplifying the task of overlaying a voice topology onto a data network. It allows network administrators to easily segment phones into separate logical networks, even though the data and voice infrastructure is physically the same—greatly simplifying the task of managing a multiservice network and identifying and troubleshooting network problems.

The Auxiliary VLAN feature maintains VLAN assignments, even when phones are moved to new locations. When a user plugs a phone into the switch, the switch provides the phone with the necessary VLAN information.

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0690
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.175
A-

AutoQoS

Network administrators can assign IP phones to separate IP subnets and VLANs to allow separate quality of service (QoS) or security policies for IP phones. By deploying AutoQoS that configures QoS on voice ports automatically, the administrative task of configuring QoS to establish end-to-end traffic prioritization is greatly simplified.

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Modules

Two classes of Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet interface modules—Classic and CEF256—provide a choice of speeds and forwarding rates (Table 4).

Classic 10/100 and 10/100/1000 Interface Modules

Suited for wiring closet applications, Classic 10/100 and 10/100/1000 modules use the supervisor's centralized forwarding engine for Layer 3 forwarding, and forward packets up to 15 Mpps.

Capable of operating in the same chassis with Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, Classic interface modules do not support distributed forwarding and cannot be upgraded with a Distributed Forwarding Card (DFC).

CEF256 10/100 and 10/100/1000 Interface Modules

Suited for premier wiring closet, distribution and core layers, data-center, and Web-hosting applications, CEF256 10/100 and 10/100/1000 interface modules use the centralized CEF engine located on the supervisor engine's policy feature card (PFC) and forward packets up to 30 Mpps.

Capable of operating in the same chassis with Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, CEF256 interface modules can also support distributed forwarding, with the following noteable exceptions: the WS-6548-GE-TX and WS-6548V-GE-TX do not support distributed forwarding.

Table 3 CEF256 10/100 and 10/100/1000 Switch Fabric DFC Upgrade Requirements

Supervisor Engine	Switch Fabric	DFC
Supervisor Engine 2 MSFC2/PFC2	Separate switch fabric module (SFM)	Requires WS-F6K-DFC upgrade
Supervisor Engine 720	Supervisor Engine 720 contains a switch fabric	Requires WS-F6K-DFC3 upgrade; will not work with WS-F6K-DFC3, or WS-F6K-DFC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0691
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.174
A.

Table 4 provides a comparison of the interface module classes available for 10/100 and 10/100/1000 Ethernet interface modules.

Table 4 Classic and CEF256 10/100 and 10/100/1000 Interface Module Comparison

Feature	Classic Interface Modules	CEF256 Interface Modules
Performance/ Forwarding Rate (Mpps)	32 Gbps; 15 Mpps per system	256 Gbps; Up to 30 Mpps per system (15 Mpps per slot for slots upgraded with DFC to support distributed forwarding)
Forwarding Engine Architecture	Supervisor engine CPU makes forwarding decision	Centralized CEF engine located on supervisor's PFCx daughter card makes forwarding decision upgradeable to dCEF switching[1] with optional WS-F6K-DFC or WS-F6K-DFC3
Supervisor Engine Supported	Supervisor Engine 1A, Supervisor Engine 2, Supervisor Engine 720	Supervisor Engine 1A, Supervisor Engine 2, Supervisor Engine 720
DFC Upgrade Requirements	Not supported	None integrated; Supervisor Engine 2—WS-F6K-DFC upgrade; SupervisorEngine 720—WS-F6K-DFC3 upgrade
Fabric Connections	32 Gbps shared bus connection (on Supervisor Engine1A, Supervisor Engine 2, and Supervisor Engine 720)	Single 8-Gbps channel connection to switch fabric [on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with Switch Fabric Module (SFM)] and 32-Gbps shared bus connection
Slot Requirements	Can occupy any slot in any chassis	Can occupy any slot in any chassis
Scheduler	Weighted Round Robin (WRR)	WRR

[1] The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support distributed forwarding; a DFCx can not be installed on these interface modules.

RQS nº 03/2005 - CN
CPMI CORREIOS
0692
Fls. Nº
3690
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.143

Cisco Catalyst Classic 10/100/1000 Voice Interface Modules

Suited for wiring closet applications, Cisco Catalyst Classic 10/100/1000 voice interface modules (Table 5) provide access to the desktop through standard RJ-45 connectors with the following operational advantages:

Forwarding architecture—Centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis— up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Time Domain Reflectometer (TDR)—Tests cabling by sending signals down the cable to identify faults in each twisted pair

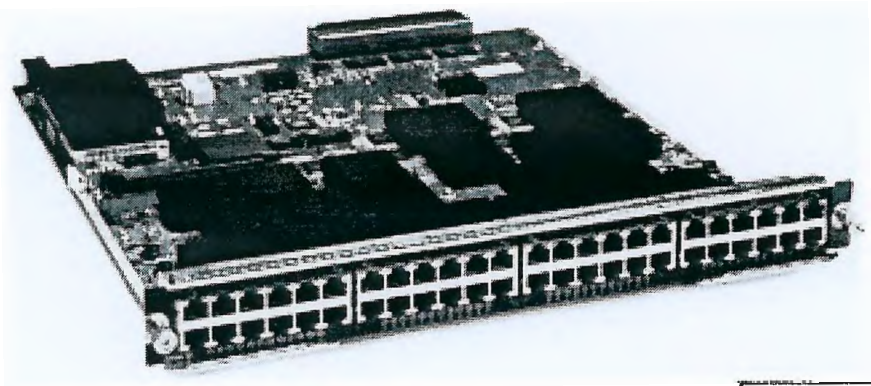
Transmit queue structure—1p2q2t = 1 strict priority queue, 2 round robin queues, 2 thresholds

Receive queue structure—1q2t = 1 round robin queue, 2 thresholds

Table 5 Classic 10/100/1000 *Voice Interface Modules*

Product	Ports/ Interface/ Connectors	Maximum Distance/ Cable Type	Maximum Frame Size (Jumbo Frame) Support	Inline Power for Voice Availability/ Upgrade Capability
WS-X6148-GE-TX	48-port;10/100/ 1000BASE-TX; RJ-45	100 meters; Category 5 cable	up to 1518 bytes	Cisco Inline Power; upgradable to 802.3af
WS-X6148V-GE-TX	48-port; 10/100/ 1000BASE-TX; RJ-45	100 meters; Category 5 cable	up to 1518 bytes	Cisco Inline Power; upgradable to 802.3af

Figure 2
Classic 10/100/1000 Voice Interface Modules
WS-X6148V-GE-TX



IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0693
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.133
A

Cisco Catalyst CEF256 10/100/1000 Voice Interface Modules

Suited for wiring closet applications, Cisco Catalyst CEF256 10/100/1000 voice interface modules provide access to the desktop through standard RJ-45 connectors and line-rate 10/100/1000 Ethernet forwarding (Table 6) with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot if upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric through one 8-Gbps connection and the 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine720

Distributed forwarding upgrade—Not Supported. The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support distributed forwarding or any DFCx.

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Time Domain Reflectometer (TDR)—Tests cabling by sending signals down the cable to identify faults in each twisted pair

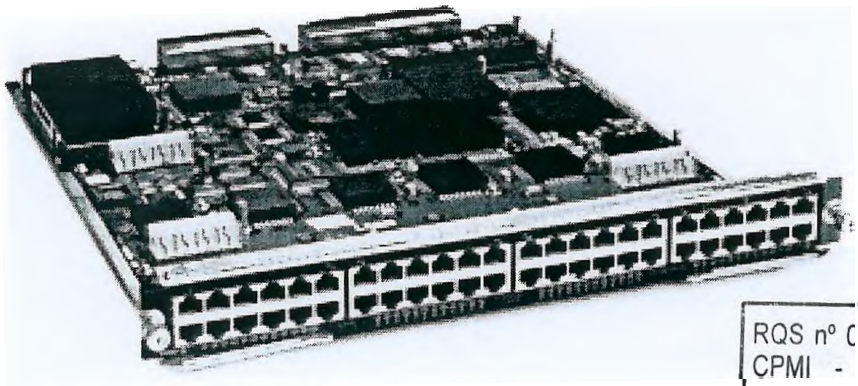
Transmit queue structure—1p2q2t = 1 priority queue, 2 round robin queues, 1 threshold

Receive queue structure—1q2t = 1 round robin queue, 2 thresholds

Table 6 *CEF256 10/100/1000 Voice Interface Modules*

Product	Ports/ Interface/ Connectors	Maximum Distance/ Cable Type	Maximum Frame Size (Jumbo Frame) Support	Inline Power for Voice Availability/ Upgrade Capability
WS-X6548-GE-TX	48-port; 10/100/ 1000BASE-TX; RJ-45	100 meters; Category 5 cable	up to 1518 bytes	Cisco Inline Power; upgradable to 802.3af

Figure 3
CEF256 10/100/1000 Voice Interface Modules
WS-X6548-GE-TX



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0694
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.111
(A.

Cisco Catalyst Classic 10/100 Copper Voice Modules

Designed for deployment in wiring closets, high-density Cisco Catalyst Classic 10/100 interface modules come with a selection of inline power capabilities and provide line-rate 10/100 Ethernet forwarding with the following operational advantages:

- Voice-ready modules with Cisco Inline Power and upgradable to 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6148-RJ45V and WS-X6148-RJ21V)
- Voice-ready modules with Cisco Inline Power and not upgradable to 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6348-RJ45V and WS-X6348-RJ21V)
- Voice-capable modules upgradable to Cisco Inline Power or 802.3af—Available in 48-port RJ-45 and RJ-21configurations (WS-X6148-RJ-45 and WS-X6148-RJ-21)

Note: These modules are designed to fully support future upgrades to the IEEE 802.3af inline power standard currently underway, providing maximum investment protection, a new daughter card will be offered once the standard is ratified.

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forwards packets up to 15 Mpps per system

Fabric connection—Connect to the switch fabric using a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Transmit queue structure—2q2t = two round robin queues and two thresholds

Receive queue structure—1q4t = one round robin queue and four thresholds

RQS nº 03/2005 - CN
CPMI - CORREIOS
0695
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

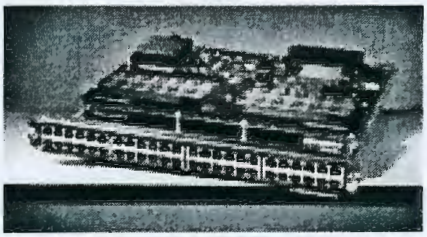
15.170
LA

Table 7 Classic 10/100 Copper Voice Interface Modules

Product	Ports/ Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support	Inline Power for Voice Availability/ Capability
WS-X6148-RJ45	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 9216 bytes	Cisco Inline Power; upgradable to 802.3af
WS-X6148-RJ21V	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 9216 bytes	Cisco Inline Power; upgradable to 802.3af
WS-X6348-RJ45V	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 8092 bytes	Cisco Inline Power; cannot upgrade to 802.3af
WS-X6348-RJ21V	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 8092 bytes	Cisco Inline Power; cannot upgrade to 802.3af
WS-X6148-RJ-45	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 9216 bytes	None provided; can upgrade to Cisco Inline Power or 802.3af
WS-X6148-RJ-21	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 9216 bytes	None provided; can upgrade to Cisco Inline Power or 802.3af

Figure 4
Classic 10/100 Copper Voice Interface Modules
WS-X6148-RJ45

VWS-X6148-RJ21V

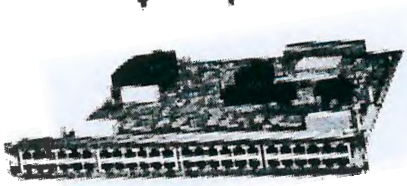


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1696
Doc. 3690

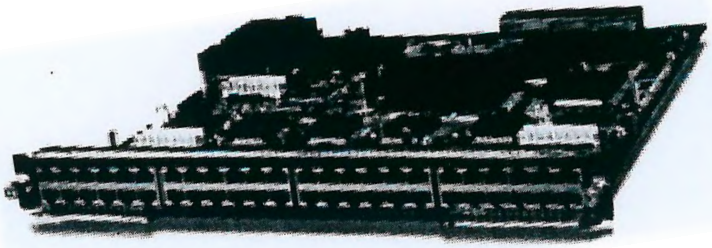
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.169
(A.

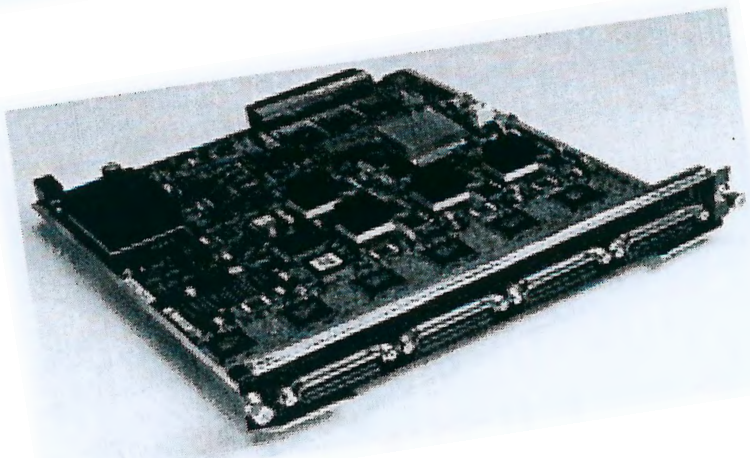
WS-X6348-RJ21V



WS-X6148-RJ-45



WS-X6148-RJ-21



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0697
3690
Doc.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.168

Cisco Catalyst CEF256 10/100 Copper Modules

Designed for small campus distribution and core layers and for data-center and Web-hosting applications where voice capability is not required, Cisco Catalyst CEF256 twisted-pair interface modules provide line-rate 10/100 Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot for slots upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric using a single 8-Gbps switch fabric channel and a 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Only required to perform distributed forwarding; require a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; require a WS-F6K-DFC upgrade to operate with Supervisor Engine 2/ MFSC2 and an SFM

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 576 ports / Cisco Catalyst 6513; up to 384 ports / Cisco Catalyst 6509

Transmit queue structure—1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

Receive queue structure—1p1q4t = 1 priority queue, 1 round robin queue, 4 thresholdse

Table 8 CEF256 Copper 10/100 Interface Modules

Product	Ports/Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support
WS-X6548-RJ-45	48-port; 10/100BASE-TX; RJ-45	100 meters; Category 5 cable	up to 9216 bytes / frame
WS-X6548-RJ-21	48-port; 10/100BASE-TX; RJ-21	100 meters; Category 5 cable	up to 9216 bytes / frame

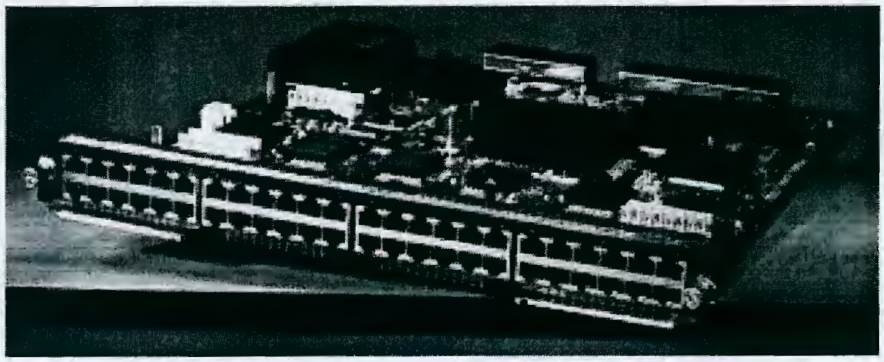
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0698
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

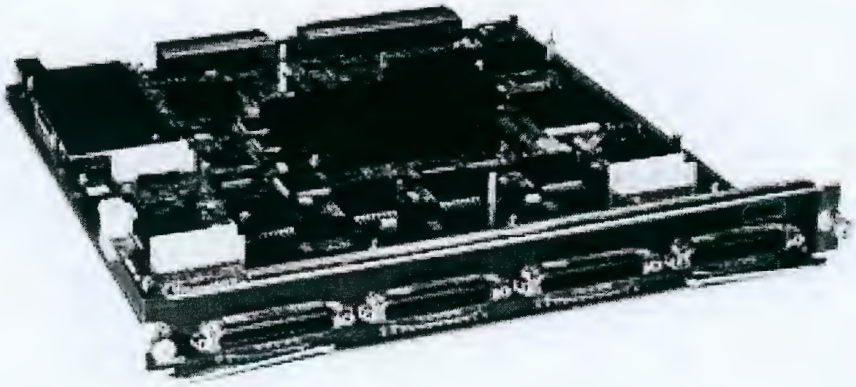
15.167
A-

Figure 5 shows high-density Cisco Catalyst CEF256 copper interface modules designed for distribution and core layers.

Figure 5
CEF256 Copper 10/100 Interface Modules
WS-X6548-RJ-45



WS-X6548-RJ-21



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0609
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.166
A.

Catalyst Classic 100FX and 10FL Fiber Interface Modules

Designed for deployment in wiring closets where optical interfaces are required, the Cisco Catalyst Classic fiber interface modules provide 10/100 Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Connect to the switch fabric using a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 288 ports / Cisco Catalyst 6513; up to 192 ports / Cisco Catalyst 6509

Transmit queue structure—2q2t = 2 round robin queues, 2 thresholds

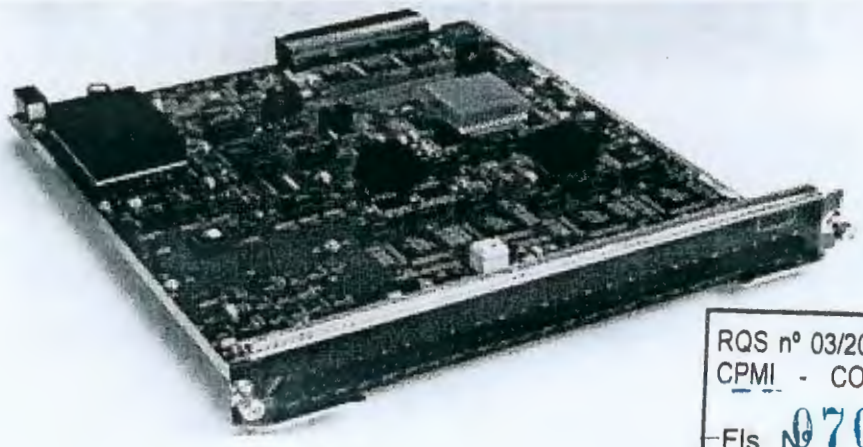
Receive queue structure—1q4t = 1 round robin queue, 4 thresholds

Note: No inline power support for voice is available for 100FX/10FL fiber modules.

Table 9 Classic 100FX/10FL Fiber Interface Modules

Product	Ports/ Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support
WS-X6324-100FX-MM	24-port; 100BASE-FX; MT-RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes / frame
WS-X6324-100FX-SM	24-port; 100BASE-FX; MT-RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes / frame
WS-X6024-10FL-MT	24-port; 10FL; MT-RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes / frame

Figure 6
Classic 100FX/10FLFiber Interface Modules
WS-X6024-10FL-MT



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0700
Doc 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.165
A.

Cisco Catalyst CEF256 100FX Fiber Modules

Designed for small campus distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst dCEF256 fiber interface modules provide line-rate 100FX Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot for slots upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric using one 8-Gbps connection and the 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Only required to perform distributed forwarding; require a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; require a WS-F6K-DFC upgrade to operate with Supervisor Engine 2/MFSC2 and a Switch Fabric Module

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Maximum Port Density / Chassis—up to 288 ports / Cisco Catalyst 6513; up to 192 ports / Cisco Catalyst 6509

Transmit queue structure—1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

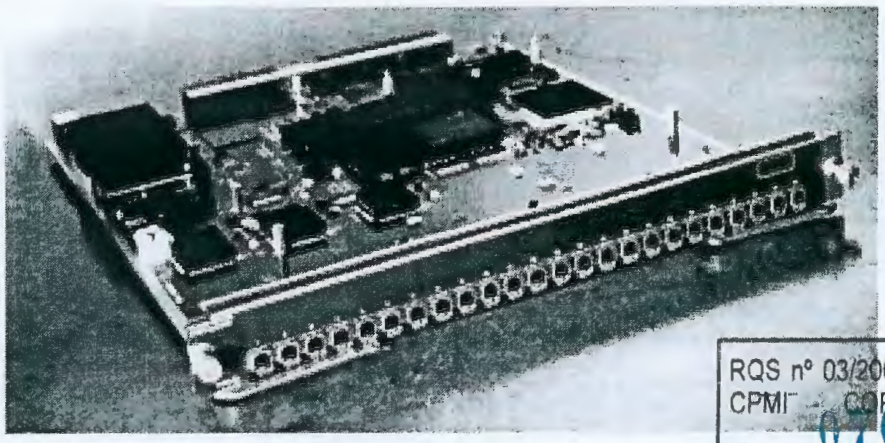
Receive queue structure—1p1q2t = 1 priority queue, 1 round robin queue, 2 thresholds

Note: No inline power support for voice is available for 100FX fiber modules.

Table 10 CEF256 100FX Fiber Interface Modules

Product	Ports/Interface/ Connectors	Maximum Distance/Cable Type	Maximum Frame Size (Jumbo Frame) Support
WS-X6524-100FX-MM	24-port; 100BASE-FX; MT- RJ	2 km; –62.5/125-micron multimode fiber; full or half duplex	up to 9216 bytes

Figure 7
CEF256 100FX Fiber Interface Modules
WS-X6524-100FX-MM



RQS nº 03/2005 - CN
CPMI - CORREIOS
0701
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.164
A-

Ordering Information

Table 11 provides part number information for Catalyst 6500 Series 10/100 and 100/1000 Ethernet interface modules.

Table 11 Catalyst 6500 Series 10/100 and 100/1000 Ethernet Interface Modules

Product Number	Description
WS-X6024-10FL-MT	Catalyst 6500 24-port 10FL Classic interface module, multimode fiber, MT-RJ
WS-X6148-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-VGE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Classic interface module; with Cisco Inline Power through voice daughter card
WS-F6K-VPWR-GE=	Catalyst 6500 Inline power daughter card (WS-X6148-GE-TX, WS-X6548-GE-TX)
WS-X6148-RJ-21	Catalyst 6500 48-port 10/100 RJ-21 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ21V	Catalyst 6500 48-port 10/100 Telco RJ-21 Classic interface module with Cisco Inline Power
WS-X6148-RJ-45	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ45V	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module with Cisco Inline Power
WS-X6348-RJ21V	Catalyst 6500 48-port 10/100 Telco RJ-21 Classic interface module with Cisco Inline Power
WS-X6348-RJ45	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module; field-upgradable to provide Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6348-RJ45V	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module with Cisco Inline Power
WS-F6K-VPWR=	Inline power daughter card to support Cisco Inline Power for Cisco Catalyst 6500 Series switches
WS-X6324-100FX-MM	Catalyst 6500 24-port 100FX Classic interface module, multimode fiber, MT-RJ
WS-X6324-100FX-SM	Catalyst 6500 24-port, 100FX Classic interface module, single-mode fiber, MT-RJ, with enhanced QoS
WS-X6548-RJ-45	Catalyst 6500 48-port, CEF256 10/100 RJ-45 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6548-RJ-21	Catalyst 6500 48-port, CEF256 10/100 RJ-21 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6516-GE-TX	Catalyst 6500 16-port 10/100/1000 RJ-45 CEF256 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6548-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 CEF256 interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR-GE=)
WS-X6548-VGE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 CEF256 interface module; with Cisco Inline Power through voice daughter card

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0702
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.163

Table 11 Catalyst 6500 Series 10/100 and 100/1000 Ethernet Interface Modules

Product Number	Description
WS-X6524-100FX-MM	Catalyst 6500 24-port, CEF256 100FX interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)

Ordering Information—DFC Daughter Cards

Table 12 provides part number information for Catalyst 6500 Series 10/100 and 100/1000 Ethernet interface modules.

Table 12 Catalyst 6500 Series 10/100 and 100/1000 Distributed Forwarding Cards

Part Number	Description
WS-F6K-DFC	Distributed forwarding card
WS-F6K-DFC=	Distributed forwarding card, spare
MEM-DFC-256MB	256-MB DRAM option for DFC
MEM-DFC-256MB=	256-MB DRAM spare option for DFC
MEM-DFC-512MB	512-MB DRAM option for DFC
MEM-DFC-512MB=	512-MB DRAM spare option for DFC
WS-F6K-DFC3A	Catalyst 6500 Dist Fwd Card-3A for 65xx, 6816 Modules
WS-F6K-DFC3A=	Catalyst 6500 Dist Fwd Card-3A for 65xx, 6816 Modules, spare

Specifications

Standard Network Protocols

- Ethernet: IEEE 802.3, 10BASE-T
- Fast Ethernet: IEEE 802.3, 100BASE-TX, and 100BASE-FX
- Gigabit Ethernet: 1000BASE-TX
- IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ad

Physical Specification

- Occupies one slot in a Cisco Catalyst 6500 Series chassis
- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Operating altitude: –60 to 4000 m

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0703
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.162

Safety Compliance

- UL 1950
- CSA-C22.2 No. 950
- EN 60950
- IEC 950
- AS/NZS 3260
- IEC 825
- EN 60825
- 21CFR1040

EMC Compliance

- FCC Part 15 (CFR 47) Class A
- VCCI Class A with UTP, Class B with STP
- EN55022 Class A with UTP, Class B with STP
- CISPR 22 Class A with UTP, Class B with STP
- CE marking
- AS/NZS 3548 Class A with UTP, Class B with STP

Network Management

- ETHERLIKE-MIB (RFC 1643)
- IF-MIB (RFC 1573)
- Bridge MIB (RFC 1493)
- CISCO-STACK-MIB
- CISCO-VTP-MIB
- CISCO-CDP-MIB
- RMON MIB (RFC 1757)
- CISCO-PAGP-MIB
- CISCO-STP-Extensions-MIB
- CISCO-VLAN-Bridge-MIB
- CISCO-VLAN-Membership-MIB
- CISCO-UDLDP-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-COPS-CLIENT-MIB
- ENTITY-MIB (RFC 2037)
- HC-RMON
- RFC1213-MIB (MIB-II)
- SMON-MIB

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0704
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.161
JA

Inline Power Specifications

- Output power per port: 48V DC power
- Pin assignment: 1, 2, 3, 6

Maximum Station-to-Station Cabling Distance

- 10/100BASE-TX, 100BASE-TX Fast Ethernet, and 10/100/1000: Category 5, 5e, and 6 UTP: 328 ft. (100 m), 100-ohm STP: 328 ft. (100 m); half or full duplex
- 100BASE-FX Fast Ethernet: 62.5/125-micron multimode fiber: 400-m half duplex, 2-km half or full duplex
- 100BASE-FX Fast Ethernet: 8/125-micron single-mode fiber: 10-km half or full duplex
- 10BASE-FL Ethernet: 62.5/125-micron multimode fiber: 2-km half or full duplex
- Maximum power: off (maximum power condition not reached); on (maximum power condition reached; no more phones will receive inline power from this module)

Indicators and Interfaces

- Status: green (operational); red (faulty); orange (module booting or running diagnostics)
- Link good: green (port active); orange (disabled); off (not active or not connected); blinking orange (failed diagnostic and disabled)
- 10/100/1000: RJ-45 (female)
- 10/100BASE-TX and 100BASE-TX: RJ-45 (female)
- 100BASE-FX: MT-RJ (female, multimode)
- 100BASE-FX: MT-RJ (female, single mode)
- 10BASE-FL: MT-RJ (female, multimode)

Cisco Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0705
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:

http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

Visit this link for to view the following data sheets:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module (CSM) Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec/VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203082/ETMG 06/02

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0706
3690
Doc.

15.159
A.

Switch Tipo 1 doc 9

RQS nº 03/2005 - CN
CPMI - CORREIOS
0707
Fls. Nº
3690
Doc.

Overview

The Catalyst 6000 family Content Switching Module (CSM) provides high-performance server load balancing (SLB) between network devices and server farms based on Layer 4 through Layer 7 packet information. Server farms are groups of real servers.

Server farms that are represented as virtual servers can improve scalability and availability of services for your network. You can add new servers and remove failed or existing servers at any time without affecting the virtual server's availability.

Clients connect to the CSM by supplying the virtual IP (VIP) address of the virtual server. When a client initiates a connection to the virtual server, the CSM chooses a real server (a physical device that is assigned to a server farm) for the connection based on configured load-balancing algorithms and policies (access rules). Policies manage traffic by defining where to send client requests for information.

Sticky connections limit traffic to individual servers by allowing multiple connections from the same client to *stick* to the same real server using source IP addresses, source IP subnets, cookies, and the secure socket layer (SSL) or by redirecting these connections using the Hypertext Transfer Protocol (HTTP) requests.

Note The CSM runs on Cisco IOS Release 12.1(6)E or later. If you are using a Supervisor Engine 2, you must use Cisco IOS Release 12.1(8a)EX or later. To use the CSM Release 2.1(1), you must be running Cisco IOS Release 12.1(8a)EX or later.
Release 2.2(1) will run with Cisco IOS Release 12.1(8a)EX. However, those features new in CSM Release 2.2(1) will not be available. To use the features added in CSM Release 2.2(1), you must be running Cisco IOS Release 12.1(11b)E or later.

Caution The WS-X6066-SLB-APC Content Switching Module is not fabric enabled.

These sections describe the CSM:

- Features, page 1-2
- Front Panel Description, page 1-4
- Operation Mode, page 1-5
- Traffic Flow, page 1-7

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0708
Doc. 3690

15.157 A.

Features

The CSM provides these enhanced features:

- More than one CSM can run in a Catalyst 6000 family switch chassis, and CSMs can run concurrently with Cisco IOS server load balancing (SLB).
- CSM fault-tolerance support allows two CSM modules (in the same or in different chassis) to be configured in the active and standby modes.
- The sticky database and connection table also can be replicated from active to standby to minimize any service disruption.
- CSM firewall load balancing allows you to scale firewall protection.
- A configurable pending-connection timeout feature is available. Pending-connection timeout sets the response time for terminating connections if a switch is flooded with traffic. This feature is used to prevent denial of service (DOS) attacks. Pending connections are configurable on a per virtual server basis.
- The CSM supports 255 VLANs.
- The minimum time between health probes has been reduced to two seconds.

Table 1-1 lists the available CSM features.

Table 1-1 CSM Feature Set Description

Features
Supported Hardware
Supervisor 1A with MSFC and PFC
Supervisor 2
Supported Protocols
TCP load balancing
UDP and all common IP protocol load balancing
Support for FTP and the Real Time Streaming Protocol (RTSP)
Layer 7 Functionality
Full regular expression matching
URL and cookie switching
Generic header parsing
Miscellaneous Functionality
Multiple CSMs in a chassis
CSM and IOS-SLB functioning simultaneously in a chassis
HTTP 1.1 persistence (all GETs to the same server)
Full HTTP 1.1 persistence (GETs balanced to multiple servers)
Fully configurable NAT
Server initiated connections

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0709
Doc. 3690

15.156
A

Table 1-1 CSM Feature Set Description (continued)

Features
Route health injection
Load-balancing Algorithms
Round robin
Weighted round robin
Least connections
Weighted least connections
URL hashing
Source IP hashing
Destination IP hashing
Configurable pending connection timeout
Load Balancing Supported
Server load balancing
Firewall load balancing
DNS load balancing
Stealth firewall load balancing
Transparent cache redirection
Reverse proxy cache
SSL off-loading
VPN-Ipsec load balancing
Stickiness
Cookie
SSL ID
Source IP
HTTP redirection
Redundancy
Sticky state
Full stateful failover (connection redundancy)
Health Checking
HTTP
ICMP
Telnet
TCP
FTP
SMTP
DNS
Return error code checking

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0710
3690
Doc

15.155 A-

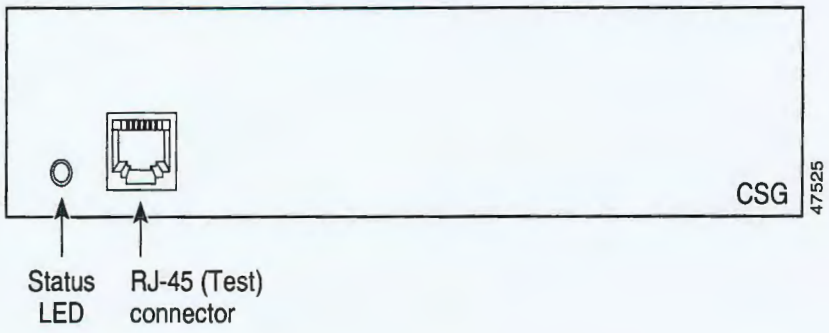
Table 1-1 CSM Feature Set Description (continued)

Features
Inband health checking
Management
SNMP traps

Front Panel Description

Figure 1-1 shows the CSM front panel.

Figure 1-1 Content Switching Module Front Panel



Note The RJ-45 connector is covered by a removable plate.

Status LED

When the CSM powers up, it initializes various hardware components and communicates with the supervisor engine. The Status LED indicates the supervisor engine operations and the initialization results.

Note For more information on the supervisor engine LEDs, refer to the *Catalyst 6000 Family Module Installation Guide*.

During the normal initialization sequence, the status LED changes from off to red, orange, and green. Table 1-2 describes the Status LED operation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0711
Doc. 3690

15.154
A

Table 1-2 Content Switching Module Status LED

Color	Description
Off	• The module is waiting for the supervisor engine to provide power. • The module is not on line. • The module is not receiving power, which could be caused by the following: – Power is not available to the CSM. – Module temperature is over the limit[1].
Red	• The module is released from reset by the supervisor engine and is booting. • If the boot code fails to execute, the LED stays red after power up.
Orange	• The module is initializing hardware or communicating with the supervisor engine. • A fault occurred during the initialization sequence. • The module has failed to download its Field Programmable Gate Arrays (FPGAs) on power up, but continues with the remainder of the initialization sequence and provides the module online status from the supervisor engine. • The module has not received module online status from the supervisor engine. This problem could be caused by the supervisor engine detecting a failure in an external loopback test that it issued to the CSM.
Green	• The module is operational; the supervisor engine has provided module online status.
Green to orange	• The module is disabled through the supervisor engine CLI [2] using the **set module disable** *mod* command.

1. Enter the **show environment temperature** *mod* command to display the temperature of each of four sensors on the CSM.
2. CLI = command-line interface.

RJ-45 Connector

The RJ-45 connector, which is covered by a removable plate, is used to connect a management station device or a test device. This connector is used by field engineers to perform testing and to obtain dump information.

Operation Mode

Clients and servers communicate through the CSM using Layer 2 and Layer 3 technology in a specific VLAN configuration. (See Figure 1-2.) Clients connect to the client-side VLAN and servers connect to the server-side VLAN. Servers and clients can exist on different subnets. Servers can also be located one or more Layer 3 hops away and connect to the server-side VLAN through routers.

A client sends a request to one of the module's VIP addresses. The CSM forwards this request to a server that can respond to the request. The server then forwards the response to the CSM, and the CSM forwards the response to the client.

When the client-side and server-side VLANs are on the same subnets, you can configure the CSM in single subnet (bridge) mode. For more information, see the "Configuring the Single Subnet (Bridge) Mode" section on page 4-2.

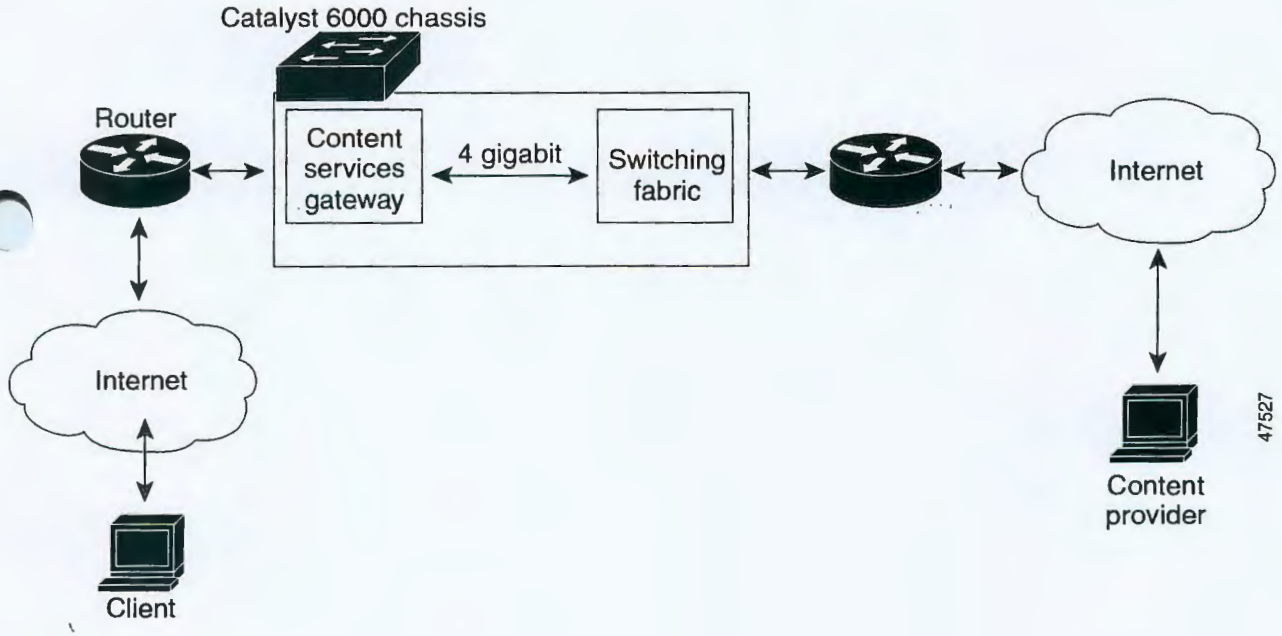
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0712
Doc. 3690

When the client-side and server-side VLANs are on different subnets, you can configure the CSM to operate in a secure (router) mode. For more information, see the "Configuring the Secure (Router) Mode" section on page 4-4.

You can set up a fault-tolerant configuration in either the secure (router) or single subnet (bridged) mode using redundant CSMs. For more information, see the "Configuring Fault Tolerance" section on page 4-5.

Using multiple VLANs, single subnet (bridge) mode and secure (router) mode can coexist in the same CSM.

Figure 1-2 Content Switching Module and Servers

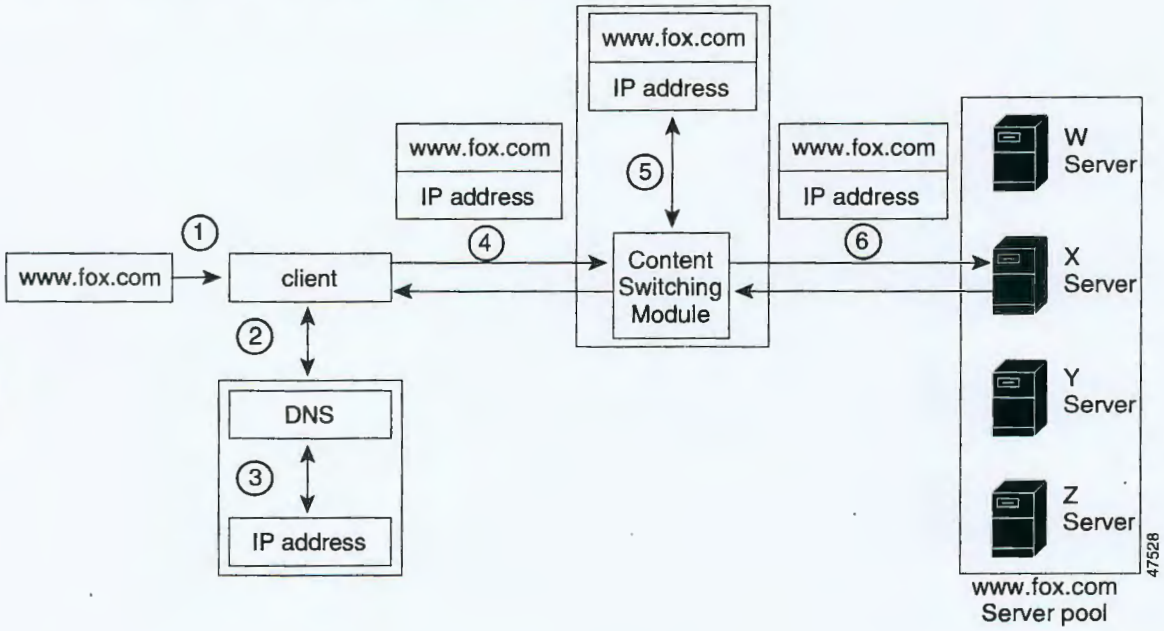


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0713
Doc. 3690

Traffic Flow

This section describes how the traffic flows between the client and server in a CSM environment. (See Figure 1-3.)

Figure 1-3 Traffic Flow between Client and Server



Note The numbers in Figure 1-3 correspond to the steps in the following operation procedure.

When you enter a request for information by entering a URL, the traffic flows as follows:

1. You enter a URL. (Figure 1-3 shows www.fox.com as an example.)
2. The client contacts a DNS server to locate the IP address associated with the URL.
3. The DNS server sends the IP address of the virtual IP (VIP) to the client.
4. The client uses the IP address (CSM VIP) to send the HTTP request to the CSM.
5. The CSM receives the request with the URL, makes a load-balancing decision, and selects a server.

   For example, in Figure 1-3, the CSM selects a server (X server) from the www.fox.com server pool, replacing its own VIP address with the address of the X server and forwards the traffic to the X server to allow the servers to initiate connections that do not have matching entries in the NAT configuration. If a NAT server is not specified, the VIP address remains unchanged.
6. The CSM performs Network Address Translation (NAT).

RQS nº 03/2005 - CN
CPMI - CORREIOS
0714
Fls. Nº
Doc. 3690

15 151

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0715
Doc. 3690

15.150
A-

Switch Tipo 1 doc 10

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0716
3690
Doc.

CHAPTER 2

Installing the Hardware

This chapter describes how to install the CSM into the Catalyst 6000 family switch and contains these sections:

- System Requirements, page 2-1
- Installing the CSM, page 2-4
- Verifying the Installation, page 2-7

System Requirements

Before you install the CSM into the Catalyst 6000 family switch, make sure the switch meets the hardware and software requirements listed in this section.

Caution You can use the MSFC, which is internal to the Catalyst 6000 family switch, to route traffic on either the client side or the server side of the CSM, but not both simultaneously.

Memory Requirements

The CSM memory is not configurable.

Supported Hardware

Before you can use the CSM, you must have a Supervisor Engine 1A with an MSFC and a Policy Feature Card (PFC) or a Supervisor Engine 2 with an MSFC, and any module that has ports to connect server and client networks.

Caution The WS-X6066-SLB-APC Content Switching Module is not fabric enabled but the module can operate in a fabric-enabled chassis like any other nonfabric module.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0717
Doc. 3690

15.148
A

The following table lists the supported hardware and software for the CSM:

Product Number	Product Description	Minimum Software Version	Recommended Software Version	Cisco IOS Release
Content Switching Module				
WS-X6066-SLB-APC with Supervisor Engine 1A	Content Switching Module	1.1(1)	2.1(1) or higher	12.1(8a)EX
WS-X6066-SLB-APC with Supervisor Engine 2	Content Switching Module	1.2(1)	2.1(1) or higher	12.1(8a)EX
WS-X6066-SLB-APC with Supervisor Engine 2	Content Switching Module	2.2(1)	2.2(1) or higher	12.1(11b)E
Console Cable				
72-876-01	Console Cable	Not applicable	Not applicable	Not applicable
Accessory Kit				
800-05097-01	Accessory kit (contains the Console Cable)	Not applicable	Not applicable	Not applicable

Power Supply

You can place the CSM in any slot in the Catalyst 6000 family chassis except for the slots occupied by the supervisor engine and the standby supervisor engine. The CSM operates on power supplied by the chassis.

Software Requirements

Caution The CSM cannot be used in a Catalyst 6000 family switch with the Catalyst operating system.

The following table lists lists the software versions for the CSM:

CSM Software Release	Software Part Number	Hardware	Cisco IOS Release	Added Features
1.1(1)	SC6k-SLB-APC-1.1	Supervisor Engine 1A with MSFC and PFC	12.1(6)E or 12.1(7)E	Initial release
1.2(1)	SC6K-1.2-CSM	Supervisor Engine 1A with MSFC and PFC or Supervisor Engine 2 Module with MSFC 2	12.1(8a)E	• Supervisor Engine 2 support • Route Health Injection (RHI)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0718
3690
Doc.

15.147
A-

CSM Software Release	Software Part Number	Hardware	Cisco IOS Release	Added Features
2.1(1)	SC6K-2.1-CSM	Supervisor Engine 1A with MSFC and PFC or Supervisor Engine 2 Module with MSFC 2	12.1(8a)EX	• Firewall load Balancing • Non-TCP load balancing • URL hashing • HTTP 1.1 persistence • Full stateful failover • Generic header parsing • SNMP server health traps • Multiple CSM in a chassis • VPN/Ipsec load balancing • Configurable NAT server
2.2(1)	SC6K-2.2-CSM	Supervisor Engine 1A with MSFC and PFC or Supervisor Engine 2 Module with MSFC 2	12.1(11b)E	• Return error code checking • Increased number of VLANs • Reduced time between health probes • Inband health checking • Configurable pending connection timeout • Real Time Streaming Protocol (RTSP) support.

Environmental Requirements

The following table lists the environmental requirements for the CSM:

Item	Specification
Temperature, ambient operating	0° to 40°C (32° to 104°F)
Temperature, ambient nonoperating	–40° to 70°C (–40° to 158°F)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Nonoperating relative humidity (noncondensing)	5% to 95%

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0719
Doc 3690

15.146
A-

Installing the CSM

The following sections describe how to install the CSM:

- Preparing to Install the CSM, page 2-4
- Preparing to Install the CSM, page 2-4
- Installing the CSM, page 2-4
- Verifying the Installation, page 2-7

Preparing to Install the CSM

Before installing the CSM, make sure that the following items are available:

- Catalyst 6000 family switch chassis
- Management station that is available through a Telnet or a console connection to perform configuration tasks

Required Tools

This section describes the tools you need to install the CSM.

Note Before installing the CSM, you must install the Catalyst 6000 family switch chassis and at least one supervisor engine. For information on installing the switch chassis, refer to the *Catalyst 6000 Family Installation Guide*.

These tools are required to install the CSM into the Catalyst 6000 family switch:

- Flat-blade screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

Installing the CSM

This section describes how to install the CSM into the Catalyst 6000 family switch.

Note All modules, including the supervisor engine (if you have redundant supervisor engines), support hot swapping. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down. For more information about hot-swapping modules, refer to the *Catalyst 6000 Family Module Installation Guide*.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0720
3690
Doc.

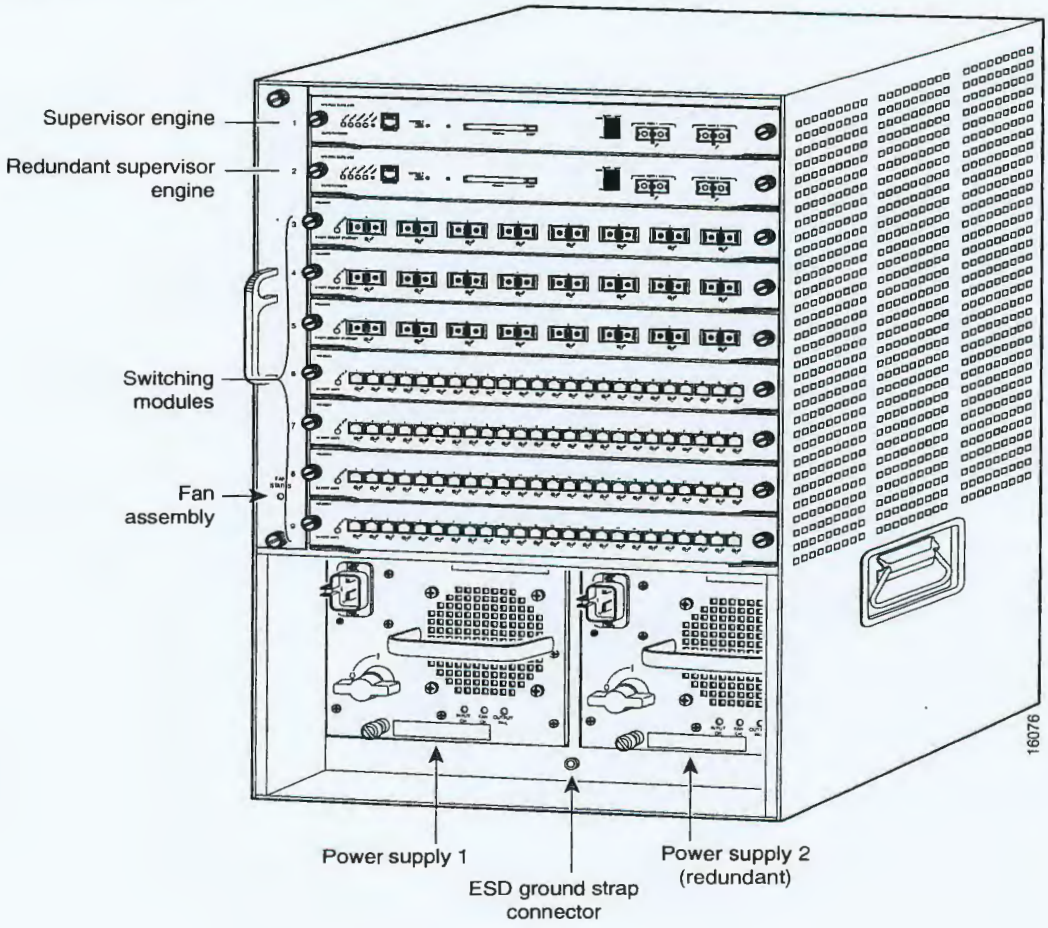
To install the CSM into the Catalyst 6000 family switch, perform these steps:

Step 1 Make sure you take the necessary precautions to prevent ESD damage.

Step 2 Choose a slot for the CSM. See Figure 2-1 for slot numbers on a Catalyst 6000 family switch.

Note Slot 1 is reserved for the supervisor engine. Slot 2 can contain an additional supervisor engine in case the supervisor engine in slot 1 fails. If a redundant supervisor engine is not required, you can insert the CSM in slots 2 through 9 on a 9-slot chassis, slots 2 through 6 on the 6-slot chassis, or slots 2 through 13 on the 13-slot chassis.

Figure 2-1 Slot Numbers on Catalyst 6000 Family Switches



Step 3 Check that there is enough clearance to accommodate any interface equipment that you will be connecting directly to the supervisor engine or switching module ports.

Note If possible, place switching modules between empty slots that contain switching-module filler plates (Cisco part number 800-00292-01).

ECT 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0721
Doc. 3890

15.144
A.

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.**

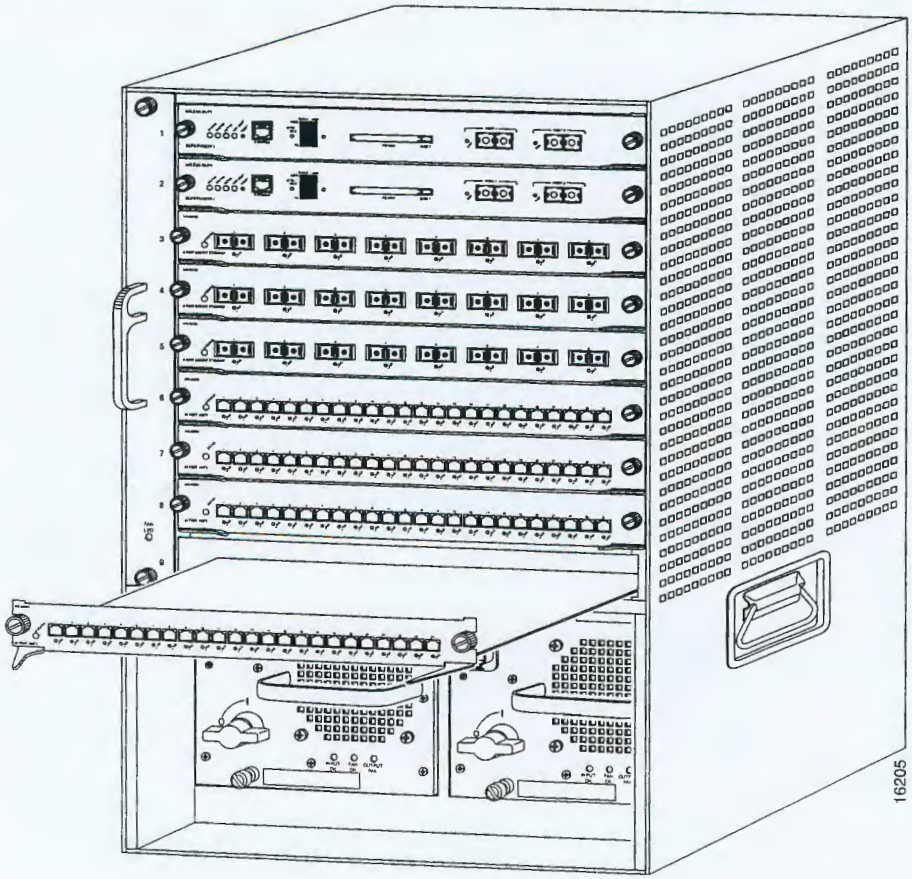
Step 4 Loosen the captive installation screws that secure the switching module filler plate (or an existing switching module) to the desired slot.

Step 5 Remove the switching module filler plate (or an existing switching module).

Step 6 Hold the handle of the CSM with one hand, and place your other hand under the carrier support. Do not touch the printed circuit boards or connector pins.

Step 7 Place the CSM in the slot. Align the notch on the sides of the switching module carrier with the groove in the slot. (See Figure 2-2.)

Figure 2-2 Installing Modules in the Catalyst 6000 Family Switch

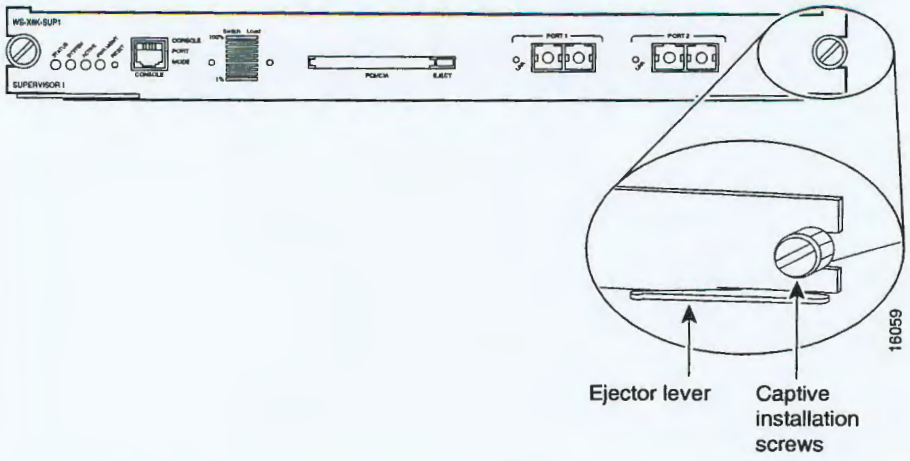


Step 8 Keep the CSM at a 90-degree angle to the backplane and carefully slide the CSM into the slot until the switching module faceplate contacts the ejector levers. (See Figure 2-3.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0722
3690
Doc.

15.143
A-

Figure 2-3 Ejector Levers and Captive Installation Screws



Step 9 Using the thumb and forefinger of each hand, simultaneously push in the left and right levers to fully seat the CSM in the backplane connector.

Caution Always use the ejector levers when installing or removing the CSM. A module that is partially seated in the backplane will cause the system to halt and subsequently crash.

Note If you perform a hot swap, the console displays the message "Module *n* has been inserted." This message does not appear, however, if you are connected to the Catalyst 6000 family switch through a Telnet session.

Step 10 Use a screwdriver to tighten the captive installation screws on the left and right ends of the CSM.

This completes the CSM installation procedure.

Verifying the Installation

When you install the CSM into the Catalyst 6000 family switch, the module goes through a boot sequence that requires no intervention. At the successful conclusion of the boot sequence, the green Status LED will light and remain on. If the Status LED does not show green, or shows a different color, refer to Table 1-2 on page 1-5 to determine the module's status.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0723
Doc. 3690

15.442
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0724
Fls. Nº
3690
Doc.

95.143
A-

Switch Tipo 1 doc 11

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0725
3690
Doc.

Configuring Content Switching

This chapter describes how to configure content switching and contains these sections:

- Configuring the Single Subnet (Bridge) Mode, page 4-2
- Configuring the Secure (Router) Mode, page 4-4
- Configuring Fault Tolerance, page 4-5
- Configuring HSRP, page 4-10

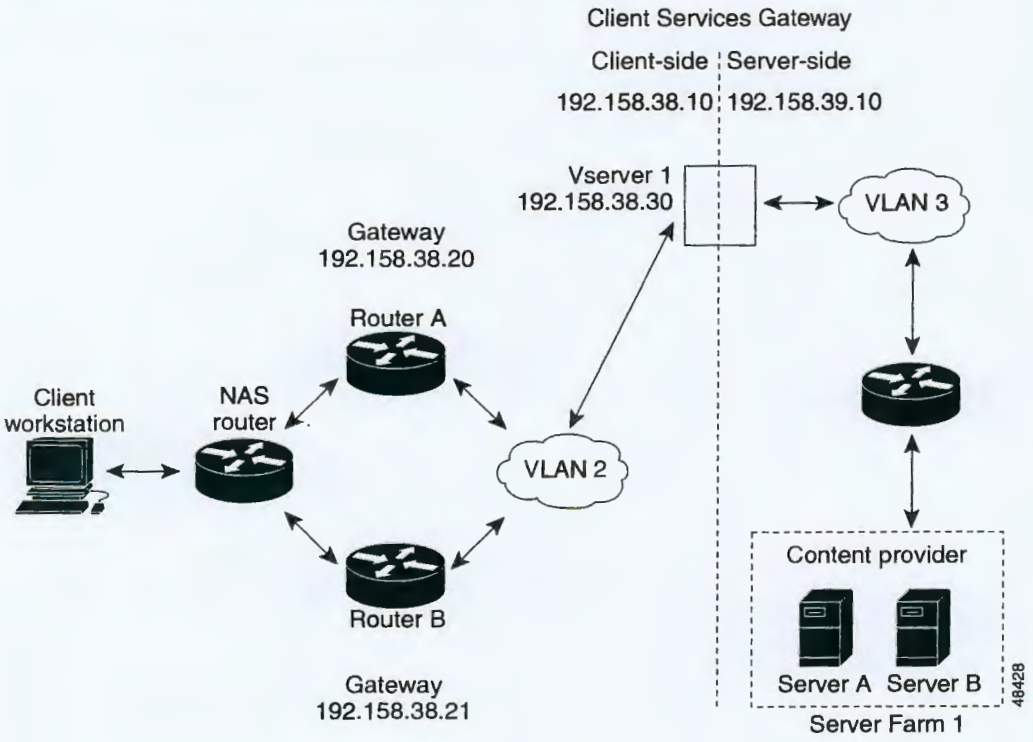
Note All examples assume that the **ip slb mode csm** command has been entered as described in Chapter 3, "Configuring the Content Switching Module."

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0726
3690
Doc.

Configuring the Single Subnet (Bridge) Mode

In the single subnet (bridge) mode configuration, the client-side and server-side VLANs are on the same subnets. Figure 4-1 shows how the single subnet (bridge) mode configuration is set up.

Figure 4-1 Single Subnet (Bridge) Mode Configuration



Note The addresses in Figure 4-1 refer to the steps in the following task table.

Note You configure single subnet (bridge) mode by assigning the same IP address to the CSM client and server VLANs.

To configure content switching for the single subnet (bridge) mode, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan database`	Enters the VLAN mode[1].
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN.
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.
Step 4	`Router(vlan)# exit`	Exits to have the configuration take effect.
Step 5	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode[1].

ECT ECT n° 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0727
3690
Doc.

15.13
A.

	Command	Purpose
Step 6	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 2.
Step 7	`Router(config-slb-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 8	`Router(config-slb-vlan-client)# gateway 192.158.38.21`	Defines the client-side VLAN gateway to Router B.
Step 9	`Router(config-slb-vserver)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 11	`Router(config-slb-vlan-client)# exit`	Exits the submode.
Step 12	`Router(config-module-csm)# vserver VIP1`	Creates a virtual server and enters the SLB *vserver* mode.
Step 13	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 14	`Router(config-slb-vserver)# serverfarm farm1`	Associates the virtual server with the server farm[3].
Step 15	`Router(config-module-csm)# inservice`	Enables the server.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.
3. This step assumes that the server farm has already been configured. See the "Configuring Server Farms" section on page 3-10.

Note Set the server's default routes to Router A's gateway (192.158.38.20) or Router B's gateway (192.158.38.21).

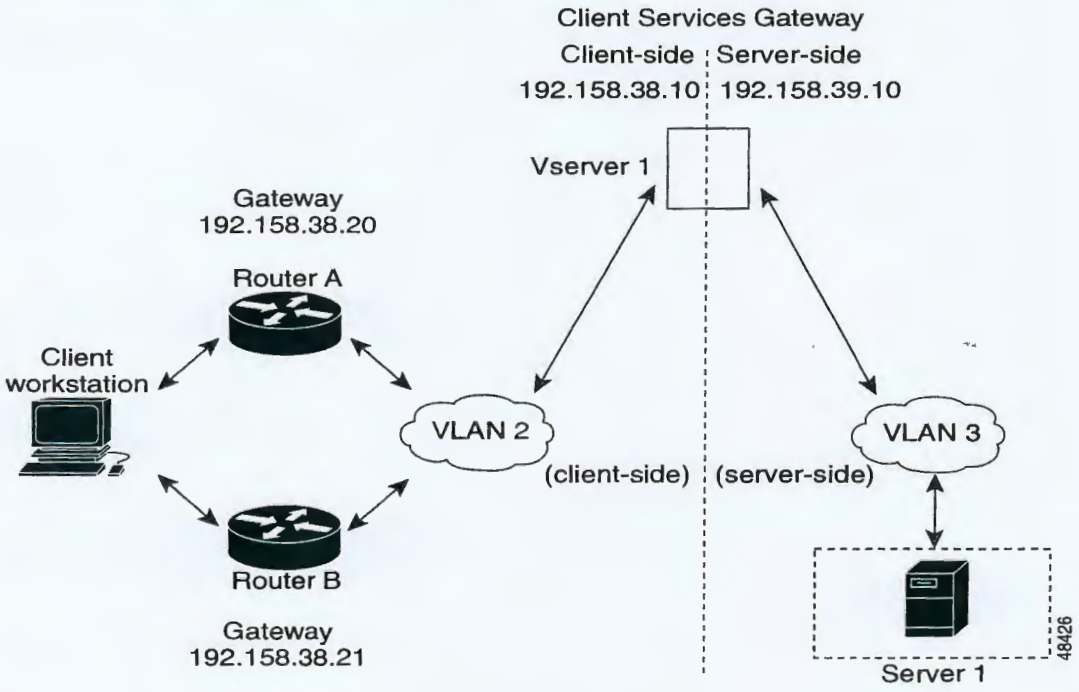
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0728
3690
Doc.

15.13.1 A.

Configuring the Secure (Router) Mode

In secure (router) mode, the client-side and server-side VLANs are on different subnets. Figure 4-2 shows how the secure (router) mode configuration is set up.

Figure 4-2 Secure (Router) Mode Configuration



Note The addresses in Figure 4-2 refer to the steps in the following task table.

To configure content switching in secure (router) mode, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan database`	Enters the VLAN mode[1].
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN[2].
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.
Step 4	`Router(vlan)# exit`	Exits to have the configuration take effect.
Step 5	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode.
Step 6	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 2.
Step 7	`Router(config-slb-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 8	`Router(config-slb-vlan-client)# gateway 192.158.38.21`	Defines the client-side VLAN gateway to Router B.

RQS n 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0720
3690
Doc.

	Command	Purpose
Step 9	`Router(config-module-csm)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	`Router(config-slb-vlan-server)# ip addr 192.158.39.10 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 11	`Router(config-slb-vlan-server)# exit`	Exits the submode.
Step 12	`Router(config-module-csm)# vserver VIP1`	Creates a virtual server and enters the SLB *vserver* mode.
Step 13	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 14	`Router(config-slb-vserver)# serverfarm farm1`	Associates the virtual server with the server farm[3].
Step 15	`Router(config-module-csm)# inservice`	Enables the server.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.
3. This step assumes that the server farm has already been configured. See the "Configuring Server Farms" section on page 3-10.

Note Set the server's default routes to the CSM's IP address (192.158.39.10).

Configuring Fault Tolerance

This section describes a fault-tolerant configuration. In this configuration, two separate Catalyst 6000 family chassis each contain a CSM.

Note You can also create a fault-tolerant configuration with two CSMs in a single Catalyst 6000 family chassis. You also can create a fault-tolerant configuration in either the secure (router) mode or nonsecure (bridge) mode.

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSM and the routers on the client side and the servers on the server side. In a redundant configuration, two CSMs perform active and standby roles. Each CSM contains the same IP, virtual server, server pool, and real server information. From the client-side and server-side networks, each CSM is configured identically. The network sees the fault-tolerant configuration as a single CSM.

Note When you configure multiple fault-tolerant CSM pairs, do not configure multiple CSM pairs to use the same FT VLAN. Use a different FT VLAN for each fault-tolerant CSM pair.

Configuring fault-tolerance requires the following:

- Two CSMs that are installed in the Catalyst 6000 family chassis.
- Identically configured CSMs. One CSM is configured as the active; the other is configured as the standby.
- Each CSM connected to the same client-side and server-side VLANs.
- Communication between the CSMs provided by a shared private VLAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0750
Fls. Nº
3690
Doc.

- A network that sees the redundant CSMs as a single entity.
- Connection redundancy by configuring a link that has a 1-GB per-second capacity. Enable the calendar in the switch Cisco IOS software so that the CSM state change gets stamped with the correct time.

  The following command enables the calendar:

```
Cat6k-2# conf t
Cat6k-2(config)# clock timezone WORD offset from UTC
Cat6k-2(config)# clock calendar-valid
```

Quality of service (QoS) configured on each CSM in the fault-tolerant pair with Cisco IOS Release 12.1(8)E and later.

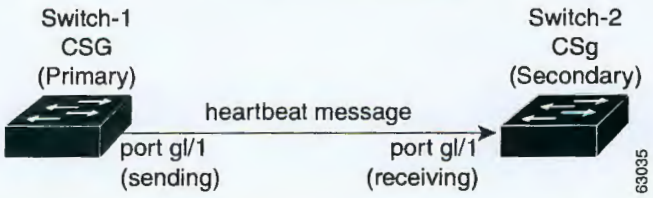
Table 4-1 lists the QoS requirements.

Table 4-1 QoS Enabling Matrix

CSM Release	Cisco IOS Release	Supervisor Engine/MSFC	Need to Configure QoS
1.1	12.1(6)E	Sup 1/MSFC or MSFC 2	No
1.1	12.1(7)E	Sup 1/MSFC or MSFC 2	No
1.2	12.1(8a)E	Sup 1/MSFC 1	No
1.2	12.1(8a)E	Sup 1/MSFC 2	No
1.2	12.1(8aE	Sup 2/MSFC 2	Yes

Figure 4-3 shows the QoS configuration topology.

Figure 4-3 QoS Configuration Topology



Without this configuration, 802.1Q priority information is not preserved in packets traversing through to the switch. Heartbeat messages sent from the active to the standby CSM must contain this priority information so that they will be transmitted without delay. When an excessive delay occurs, an unnecessary takeover might occur.

You can overcome this limitation by configuring the sending port g1/1 to retain priority information upon transmission and the receiving port g1/1 to trust the class of service (CoS) (priority bits) for the incoming packets.

The **permit any any** command informs the switch to accept incoming packets with any MAC address from any MAC address.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0731
3690
Doc.

15.134
34

To configure QoS for a fault-tolerant configuration, enter these commands:

```
Cat6k-2(config)# mls qos
Cat6k-2(config)# interface g1/1
Cat6k-2(config-if)# no shutdown
Cat6k-2(config-if)# mls qos cos 7
Cat6k-2(config-if)# switchport
Cat6k-2(config-if)# switchport access vlan 200
Cat6k-2(config-if)# switchport trunk encapsulation dot1q
Cat6k-2(config-if)# switchport trunk allowed vlan 1,2,1002-1005
Cat6k-2(config-if)# switchport mode trunk
```

Table 4-2 lists CSM fault-tolerant configuration requirements.

Table 4-2 CSM Fault-tolerant Configuration Requirements

Configuration Parameter	On Both Content Switching Modules	
	Same	Different
VLAN name	X	
VLAN address		X
Gateway[1] address	X	
Virtual server name	X	
Virtual IP address	X	
Alias IP addresses	X	
Redundancy group name	X	
Redundancy VLAN ID	X	

1. Server default gateways must point to the alias IP address.

Because each CSM has a different IP address on the client-side and server-side VLAN, the CSM can issue health monitor probes (see the "Configuring Probes for Health Monitoring" section on page 6-1) to the network and receive responses. Both the active and standby CSMs send probes while operational. If the passive CSM assumes control, it knows the status of the servers because of the probe responses it has received.

Enter the **replicate csrp {sticky | connection}** command in the virtual server mode to configure replication for the CSMs.

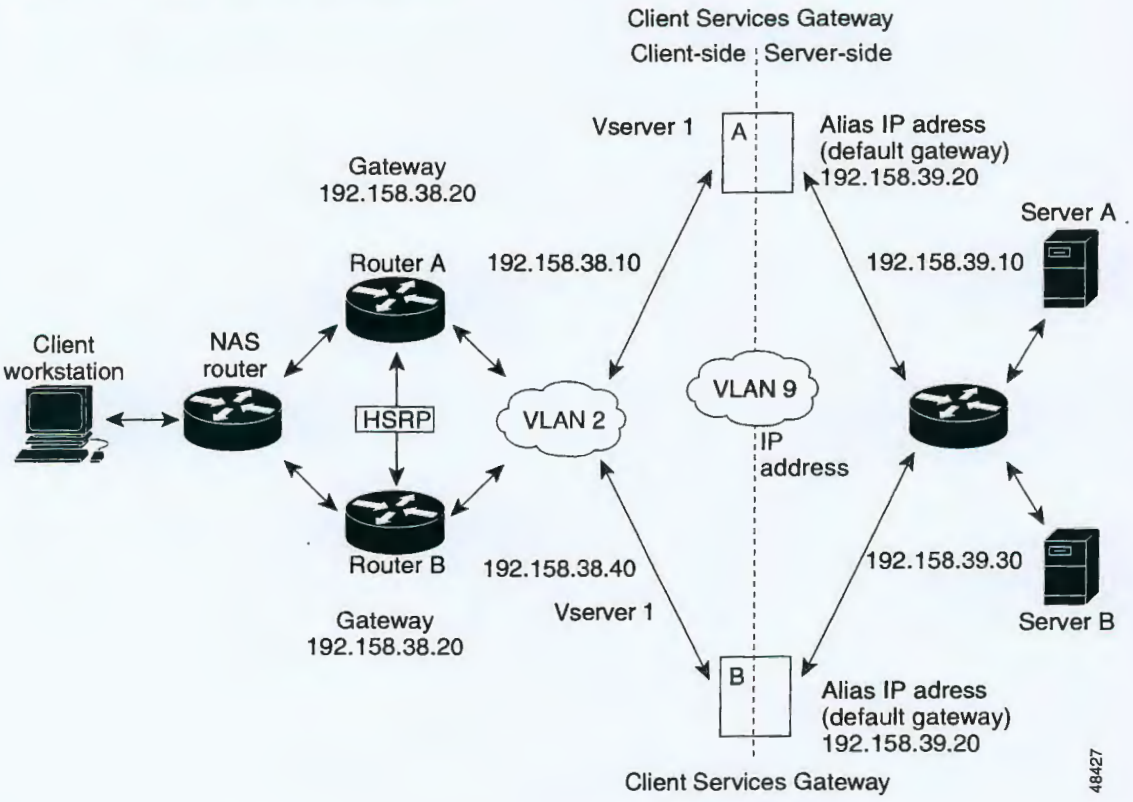
Note The default setting for the **replicate** command is disabled.

If no router is present on the server-side VLAN, then each server's default route points to the aliased IP address.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0732
Fls. Nº
3690
Doc.

Figure 4-4 shows how the secure (router) mode fault-tolerant configuration is set up.

Figure 4-4 Fault-Tolerant Configuration



Note The addresses in Figure 4-4 refer to the steps in the following two task tables.

To configure the active (A) CSM for fault tolerance, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode[1].
Step 2	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the content switching IP address on VLAN 1.
Step 3	`Router(config-slb-vlan-client)# gateway 192.158.38.20 255.255.255.0`	(Optional) Defines the client-side VLAN gateway for an HSRP enabled gateway.
Step 4	`Router(config-module-csm)# vserver vip1`	Creates a virtual server and enters the SLB vserver mode.

ROS nº 03/2005 - CN
CPMI - CORREIOS
0783
Doc. 3690

15.132

	Command	Purpose
Step 5	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 6	`Router(config-module-csm)# inservice`	Enables the server.
Step 7	`Router(config-module-csm)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 8	`Router(config-slb-vserver)# ip addr 192.158.39.10 255.255.255.0`	Assigns the CSM IP address on VLAN 2.
Step 9	`Router(config-slb-vserver)# alias ip addr 192.158.39.20 255.255.255.0`	Assigns the default route for VLAN 2.
Step 10	`Router(config-module-csm) vlan 9 ft`	Defines VLAN 9 as a fault-tolerant VLAN.
Step 11	`Router(config-module-csm)# ft group` *ft-group-number* `vlan 9`	Creates the content switching active and standby (A/B) group VLAN 9.
Step 12	`Router(config-module-csm)# vlan database`	Enters the VLAN mode[1].
Step 13	`Router(vlan)# vlan 2`	Configures a client-side VLAN 2[2].
Step 14	`Router(vlan)# vlan 3`	Configures a server-side VLAN 3.
Step 15	`Router(vlan)# vlan 9`	Configures a fault-tolerant VLAN 9.
Step 16	`Router(vlan)# exit`	Enters the **exit** command to have the configuration take affect.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.

To configure the standby (B) CSM for fault tolerance, perform this task (see Figure 4-4):

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode[1].
Step 2	`Router(config-slb-vlan-client)# ip addr 192.158.38.40 255.255.255.0`	Assigns the Content Switching IP address on VLAN 2.
Step 3	`Router(config-module-csm) vlan 9 ft`	Defines VLAN 9 as a fault-tolerant VLAN.
Step 4	`Router(config-slb-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway.
Step 5	`Router(config-module-csm)# vserver vip1`	Creates a virtual server and enters the SLB *vserver* mode.
Step 6	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 7	`Router(config-module-csm)# inservice`	Enables the server.
Step 8	`Router(config-module-csm)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB *vlan* mode.
Step 9	`Router(config-slb-vserver)# ip addr 192.158.39.30 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 10	`Router(config-slb-vserver)# alias 192.158.39.20 255.255.255.0`	Assigns the default route for VLAN 2.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0734
3690
Doc.

	Command	Purpose
Step 11	`Router(config-module-csm)# ft group ft-group-number vlan 9`	Creates the CSM active and standby (A/B) group VLAN 9.
Step 12	`Router(config-module-csm)# show module csm ft`	Displays the state of the fault tolerant system.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.

Configuring HSRP

This section provides an overview of a Hot Standby Router Protocol (HSRP) configuration (see Figure 4-5) and describes how to configure the CSMs with HSRP and CSM failover on the Catalyst 6000 family switches.

HSRP Configuration Overview

Figure 4-5 shows that two Catalyst 6000 family switches, Switch 1 and Switch 2, are configured to route from a client-side network (10.100/16) to an internal CSM client network (10.6/16, VLAN 136) through an HSRP gateway (10.100.0.1). The configuration shows the following:

- The client-side network is assigned an HSRP group ID of HSRP ID 2.
- The internal CSM client network is assigned an HSRP group ID of HSRP ID 1.

Note HSRP group 1 must have tracking turned on so that it can track the client network ports on HSRP group 2. When HSRP group 1 detects any changes in the active state of those ports, it duplicates those changes so that both the HSRP active (Switch 1) and HSRP standby (Switch 2) switches share the same knowledge of the network.

In the example configuration, two CSMs (one in Switch 1 and one in Switch 2) are configured to forward traffic between a client-side and a server-side VLAN:

- Client VLAN 136

Note The client VLAN is actually an internal CSM VLAN network; the actual client network is on the other side of the switch.

- Server VLAN 272

  The actual servers on the server network (10.5/1) point to the CSM server network through an aliased gateway (10.5.0.1), allowing the servers to run a secure subnet.

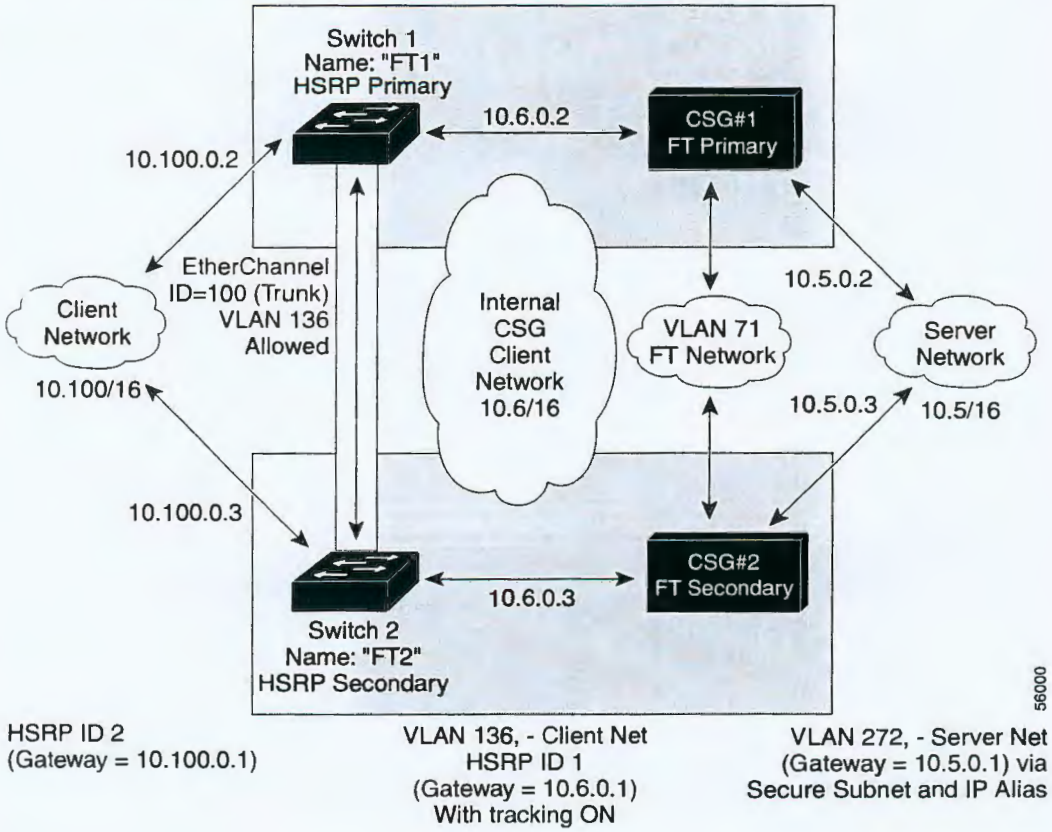
  In the example configuration, an EtherChannel is set up with trunking enabled, allowing traffic on the internal CSM client network to travel between the two Catalyst 6000 family switches. The setup is shown in Figure 4-5.

Note EtherChannel protects against a severed link to the active switch and a failure in a non-CSM component of the switch. EtherChannel also provides a path between an active CSM in one switch and another switch, allowing CSMs and switches to fail over independently, providing an extra level of fault tolerance.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0735
Fls. Nº
3690
Doc.

15.130
A

Figure 4-5 HSRP Configuration



Creating the HSRP Gateway

This procedure describes how to create an HSRP gateway for the client-side network. The gateway is HSRP ID 2 for the client-side network.

Note In this example, HSRP is set on Fast Ethernet ports 3/6.

To create an HSRP gateway, follow these steps:

Step 1 Configure Switch 1—FT1 (HSRP active) as follows:

```
Router(config)#interface FastEthernet3/6
Router(config)#ip address 10.100.0.2 255.255.0.0
Router(config)#standby 2 priority 110 preempt
Router(config)#standby 2 ip 10.100.0.1
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0736
Doc. 3690

Step 2 Configure Switch 2—FT2 (HSRP standby) as follows:

```
Router(config)#interface FastEthernet3/6
Router(config)#ip address 10.100.0.3 255.255.0.0
Router(config)#standby 2 priority 100 preempt
Router(config)#standby 2 ip 10.100.0.1
```

Creating Fault-Tolerant HSRP Configurations

This section describes how to create a fault-tolerant HSRP secure-mode configuration. To create a nonsecure-mode configuration, enter the commands described with these exceptions:

- Assign the same IP address to both the server-side and the client-side VLANs.
- Do not use the **alias** command to assign a default gateway for the server-side VLAN.

To create fault-tolerant HSRP configurations, follow these steps:

Step 1 Configure VLANs on HSRP FT1 as follows:

```
Router(config)# module csm 5
Router(config-module-csm)# vlan 136 client
Router(config-slb-vlan-client)# ip address 10.6.0.245 255.255.0.0
Router(config-slb-vlan-client)# gateway 10.6.0.1
Router(config-slb-vlan-client)# exit

Router(config-module-csm)# vlan 272 server
Router(config-slb-vlan-server)# ip address 10.5.0.2 255.255.0.0
Router(config-slb-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-slb-vlan-server)# exit

Router(config-module-csm)# vlan 71 ft

Router(config-module-csm)# ft group 88 vlan 71
Router(config-slb-ft)# priority 30
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit

Router(config-module-csm)# interface Vlan136
ip address 10.6.0.2 255.255.0.0
standby 1 priority 100 preempt
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

Step 2 Configure VLANs on HSRP FT2 as follows:

```
Router(config)# module csm 6
Router(config-module-csm)# vlan 136 client
Router(config-slb-vlan-client)# ip address 10.6.0.246 255.255.0.0
Router(config-slb-vlan-client)# gateway 10.6.0.1
Router(config-slb-vlan-client)# exit

Router(config-module-csm)# vlan 272 server
Router(config-slb-vlan-server)# ip address 10.5.0.3 255.255.0.0
Router(config-slb-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-slb-vlan-server)# exit

Router(config-module-csm)# vlan 71 ft
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0737
Doc. 3690

```
Router(config-module-csm)# ft group 88 vlan 71
Router(config-slb-ft)# priority 20
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit

Router(config-module-csm)# interface Vlan136
ip address 10.6.0.3 255.255.0.0
standby 1 priority 100 preempt
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

Note To allow tracking to work, preempt must be on.

Step 3 Configure EtherChannel on both switches as follows:

```
Router(console)# interface Port-channel100
Router(console)# switchport
Router(console)# switchport trunk encapsulation dot1q
Router(console)# switchport trunk allowed vlan 136
```

Note By default, all VLANs are allowed on the port channel.

To prevent problems, remove the server and FT CSM VLANs as follows:

```
Router(console)# switchport trunk remove vlan 71
Router(console)# switchport trunk remove vlan 272
```

Step 4 Add ports to the EtherChannel as follows:

```
Router(console)# interface FastEthernet3/25
Router(console)# switchport
Router(console)# channel-group 100 mode on
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0738
Doc. 3690

15.120
A.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0739
Doc. 3690

15.125
CA

Switch Tipo 1 doc 12

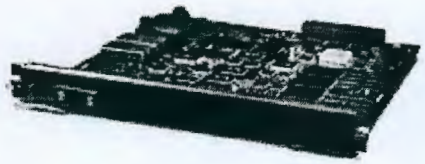
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0740
Doc 3690

Cisco Systems

15.124 A.

Data Sheet

Cisco **Catalyst 6500** Series Content Switching Module

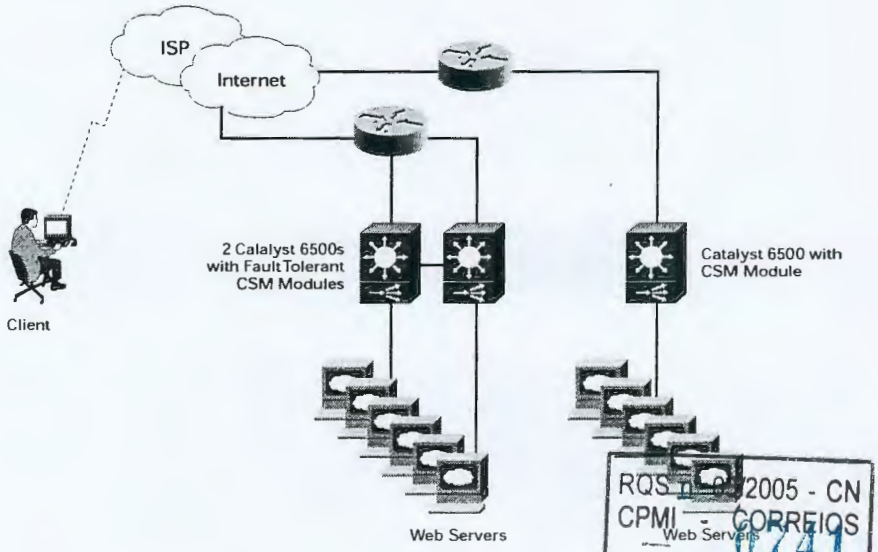


The Cisco Content Switching Module (CSM) is a Cisco Catalyst® 6500 line card that balances client traffic to farms of servers, firewalls, Secure Sockets Layer (SSL) devices, or virtual private network (VPN) termination devices. The Cisco CSM provides a high-performance, cost-effective load-balancing solution for enterprise and Internet service provider (ISP) networks. The Cisco CSM meets the demands of high-speed content delivery networks, tracking network sessions and server load conditions in real time and directing each session to the most appropriate server. Fault-tolerant Cisco CSM configurations maintain full state information and provide true hitless failover required for mission-critical functions.

The Cisco CSM provides the following key benefits (refer to Figure 1):

- Market-leading performance—The Cisco CSM establishes up to 165,000 Layer 4 connections per second (depending on software version) and provides high-speed content switching while maintaining 1 million concurrent connections.
- Outstanding price/performance value for large data centers and ISPs—The Cisco CSM features a low connection cost and occupies a small footprint. It slides into a slot in a new or existing Cisco Catalyst 6500 and enables all ports in the Cisco Catalyst 6500 for Layer 4–7 content switching.
- Multiple Cisco CSMs can be installed in the same Cisco Catalyst 6500.
- Ease of configuration—The Cisco CSM uses the same Cisco IOS® command-line interface (CLI) that is used to configure the Cisco Catalyst 6500 Switch.

Figure 1. The Cisco CSM



RQS nº 2005 - CN
CPMI - CORREIOS
0741
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.123
A-

Content Switching Module Key Features

Firewall Load Balancing

The Cisco CSM allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis, while ensuring that all packets belonging to a particular connection go through the same firewall. Both stealth and regular firewalls are supported.

URL and Cookie-Based Load Balancing

The Cisco CSM allows full regular expression pattern matching for policies based on URLs, cookies, and Hypertex Transfer Protocol (HTTP) header fields. The Cisco CSM supports any URL or cookie format—allowing it to load balance existing Web content without requiring URL/cookie format changes.

High Performance

The Cisco CSM performs up to 165,000 new Layer 4 TCP connection setups per second, depending on software version. These connections can be spread across 4096 virtual servers (16,384 real servers) and all the ports in a Cisco Catalyst 6500, or they can be focused on a single port. This provides a benefit over competitors who use distributed architectures that require use of all the ports in order to gain maximum performance.

Network Configurations

The Cisco CSM supports many different network topology types. A Cisco CSM can operate in a mixed bridged and routed configuration, allowing traffic to flow from the client side to the server side on the same or on different IP subnets.

IP Protocol Support

The Cisco CSM accommodates a wide range of common IP protocols—including TCP and User Datagram Protocol (UDP). Additionally, the Cisco CSM supports higher-level protocols, including HTTP, File Transfer Protocol (FTP), Telnet, Real-Time Streaming Protocol (RTSP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP).

User Session Stickiness

Whenever encryption or e-commerce is involved, it is important that the end user is consistently directed to the same server-that is, the server where the user's shopping cart is located or the encryption tunnel terminates. Cisco CSM User Session Stickiness provides the ability to consistently bring users back to the same server-based on SSL session ID, IP address, cookie, or HTTP redirection.

Load-Balancing Algorithms

The Cisco CSM supports the following load-balancing algorithms:

- Round robin
- Weighted Round Robin
- Least connections
- Weighted least connections
- Source and/or destination IP hash (subnet mask also configurable)
- URL hashing

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0742
Fls. Nº
Doc. 3690

15.122
A.

Quality of Service

Providing differentiated levels of service to end users is important when generating revenue from content. The Cisc CSM takes advantage of the robust quality of service (QoS) of the Cisco Catalyst 6500, enabling traffic differentiation as follows:

- Correctly prioritizes packets based on Layer 7 rules
- Directs users who are paying more for services to faster or less loaded servers

High Availability

The Cisco CSM continually monitors server and appliation availability using health monitoring probes, inband health monitoring, return code checking, and the Dynamic Feedback Protocol (DFP). When a real server or gatewa failure occurs, the Cisco CSM redirects traffic to a different location. Servers can be added and removed without disrupting service—systems can easily be scaled up or down.

Connection Redundancy

Optionally, two Cisco CSMs can be configured in a fault-tolerant configuration to share state information about use sessions and provide connection redundancy. If the active Cisco CSM fails, open connections are handled by the standby CSM without interruption, and users experience hitless failover—an important requirement for e-commerc sites and sites where encryption is used.

Global Server Load Balancing

The CSM offers multiple options for building a global or geographical load balanced environment. The CSM can act as an authoritative DNS and perform GSLB among geographically dispersed CSMs for the purposes of disaster recovery or for small GSLB environments with 2-4 locations. In addition, the CSM can report load information for it's Virtual IPs into the Global Site Selector (GSS), an appliance designed for advanced GSLB scaling up to 128 sites. With the many different GSLB options the CSM offers the ability to scale GSLB capabilities as growth demands.

Configuration Limits

- Total virtual LANs (VLANs) (client and server): 256
- Virtual servers: 4000
- Server farms: 4000

RQS nº 03/2005 - CN
GPMI - CORREIOS
0743
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.121
A-

- Real servers: 16,000
- Probes: 4000
- Access control list (ACL) items: 16,000

Performance Summary
Connections
1,000,000 concurrent TCP connections
165,000 connection setups per second—Layer 4
Throughput
Total combined throughput of 4 Gigabits per second (client to server and server to client)
Cisco Catalyst Switch Platform Requirements
Cisco IOS Software only—Cisco Catalyst Operating System is not supported
Not fabric enabled—Functions as a bus-enabled line card
Multilayer Switch Feature Card (MSFC) or MSFC2
Physical Specifications
Occupies slot in the Cisco Catalyst 6500 chassis
Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)
Weight: 5 lb (2.27 kg)
Operating Environment
Operating temperature: 32 to 104.5°F (0 to 40°C)
Nonoperating temperature: –40 to 158°F (–40 to 70°C)
Operating relative humidity: 10 to 90% (noncondensing)
Nonoperating relative humidity: 5 to 95% (noncondensing)
Operating and nonoperating altitude: Sea level to 10,000 ft (3050m)
Agency Approvals
Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS NZS 3548 Class A
Safety: CE Marking according to UL 1950, CSA 22.2 No. 950, EN 60950, IEC 60950, TS 001, AS/NZS 3260

Cisco Catalyst 6500 CSM Ordering Information

Product Number	Product Description
WS-X6066-SLB-APC	Cisco Catalyst 6500 Content Switching Module

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0744
Doc. 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-120
SA.

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

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Printed in the USA

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0745
3690
Doc.

15.113
A

Switch Tipo 1 doc 13

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0746
3690
Doc.

CiscoWorks CiscoView 5.4

15.118
A.

THE CISCOVIEW DEVICE MANAGER IS THE MOST WIDELY DEPLOYED DEVICE MANAGEMENT SOFTWAI APPLICATION PROVIDED BY CISCO. BEING WEB-BASED, CISCOWORKS CISCOVIEW ALLOWS UBIQUITOU ACCESS FROM ANY CLIENT WITH A STANDARD BROWSER, NETWORK ACCESS, AND MINIMUM HARDWAI REQUIREMENTS. USERS CONTINUE TO RELY ON THE INTUITIVE INTERFACE, REAL-TIME DEVICE MONITORIN AND EASY DEVICE CONFIGURATION IN CISCOVIEW, AS WELL AS NEW FEATURES THAT ENHANCE IT FUNCTIONALITY. EASILY INTEGRATED WITH CISCOWORKS PRODUCTS OR PARTNER PLATFORMS, CISCOVIE PROVIDES MULTI-USER DEVICE MANAGEMENT IN THE LARGER CONTEXT OF AN END-TO-END MANAGEMEN INTRANET SOLUTION.

CiscoView Web-based management aides network management by displaying a physical view of Cisco devices and color-coding device ports for at-a-glance port status, allowing users to quickly grasp essential information. CiscoView features provide dynamic status, device monitoring, and comprehensive configuration information for Cisco internetworking products (routers, switches, and access products). Features include:

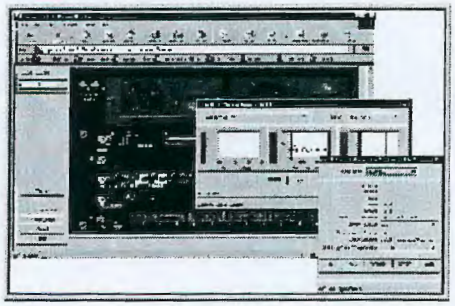
- Web-based displays of Cisco products from a single location, giving network managers a complete view of Cisco products without physically checking each device (see Figure 1)
- A continuously updated physical view of routers, hubs, switches, or access servers in a network
- Real-time monitoring and tracking of key information and data relating to device performance, traffic, and environment, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators
- The ability to modify device configurations across router, switch, and access server products.
- The ability to access the support for existing and new Cisco devices via the Web-based Package Support Updater (PSU), without having to purchase and install new versions of CiscoView
- Multi-user access to a single CiscoView server through a Web-based client

New CiscoView 5.4 Features

CiscoView 5.4 has several new features including:

- New device support
- Secure communication between the client browser and the server via Secure Sockets Layer (SSL) protocol
- Device list import from local RME through SSL

Figure 1 CiscoView 5



Common Management Foundation

CiscoView 5.4 uses many of the components in the CiscoWorks common management foundation. An integration utility is available to all CiscoWorks applications to provide integration with third-party network management systems (NMSs). This utility adds CiscoView device-specific information to the NMS and provides launch points to other Cisco applications, creating a seamless management environment for the end user. The utility's modular, independent design allows:

- Integration between applications residing on different servers and even different operating systems
- Dynamic updates to integration information in the NMS
- Dynamic upgrades to new versions of the NMS, without reinstalling CiscoWorks
- Flexibility in customizing your management intranet environment using totally Web-based tools from Cisco

NMS support is updated frequently, and files can be downloaded from CCO by referring to the CiscoView planner page: http://www.cisco.com/cgi-bin/Software/Cisco_dev/vplanner.cgi

CISCO SYSTEMS

ROS nº 03/2005 - CN
CPMI - CORREIOS
0747
Fls. Nº
3690
Doc.

15.117

More Information

For more information on CiscoView see the CiscoView Upgrade Planner at http://www.cisco.com/public/sw-center/sw-netmgmt.shtml Server, Client, and Web Browser Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions, and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Device Support

The modular design of CiscoView allows users to add support for devices as necessary. Device support files can be downloaded through the Web-based CiscoView Package Support Updater (PSU), located on the CiscoWorks desktop. The PSU is used for scheduled and on-demand device support downloads from CCO. To find more information on downloading device packages, please click on this URL:. http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cvparnt/cview/cv4gsg/cvgsdld.htm#xtocid238445

To get the most recent list of devices supported, see: http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi

Ordering Information

CiscoView is sold as an integral part of several Cisco solutions, and is not sold as an individual product.

The Routed WAN Management Solution and the LAN Management Solution contain CiscoView, as does CiscoWorks for Windows.

Availability

CiscoView is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For more information on CiscoView and on the CiscoWorks family of products, see: http://cisco.com/warp/public/cc/pd/wr2k/

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0748
Doc. 3690

15. 116
4.

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

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: 61 2 8448 7100
Fax: 61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000, Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0007R)

0909 BW6024

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0749
3690
Doc.

15.115
L4.

Switch Tipo 2 doc 1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0750
Doc. 3690

Cisco Systems

15.114
A.

Data Sheet

Cisco Catalyst 2950 Series Switches with Cisco **Enhanced** Image Software

Product Overview

Cisco® Catalyst® 2950 Series switches are fixed-configuration, stackable models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for small and medium-sized networks. The Cisco Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge—while maintaining the simplicity of traditional LAN switching. When a Cisco Catalyst 2950 Series Switch is combined with a Cisco Catalyst 3550 Series Switch, the solution can enable IP routing from the edge to the core of the network. Embedded in Cisco Catalyst 2950 Series switches is Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Cisco Catalyst desktop switches using a standard Web browser. In addition to Cisco CMS Software, Cisco Catalyst 2950 Series switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks.

This product line offers two distinct sets of software features and several configurations to allow small, medium-sized, and enterprise branch offices to select the right combination for the network edge. Cisco Standard Image (SI) Software offers Cisco IOS® Software functioning for basic data, video, and voice services. For networks with requirements for additional security, advanced QoS, and high availability, the Cisco Enhanced Image (EI) Software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge.

The Cisco Catalyst 2950 Series switches consists of the following devices—which are only available with Cisco EI Software for the Cisco Catalyst 2950 Series.

- Catalyst 2950G-48—48 10/100 ports and 2 Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports
- Catalyst 2950G-24—24 10/100 ports and 2 GBIC ports
- Catalyst 2950G-24-DC—24 10/100 ports, 2 GBIC ports, and DC power
- Catalyst 2950G-12—12 10/100 ports and 2 GBIC ports
- Catalyst 2950T-24—24 10/100 ports and 2 fixed 10/100/1000BASE-T uplink ports
- Catalyst 2950C-24—24 10/100 ports and 2 fixed 100BASE-FX uplink ports

This complete set of switches offers network managers flexibility when selecting a migration path to Gigabit Ethernet. The two built-in Gigabit Ethernet ports on the Cisco Catalyst 2950G-12, 2950G-24, and 2950G-48 accommodate a range of GBIC transceivers, including the Cisco GigaStack® GBIC, as well as 1000BASE-SX, 1000BASE-LX/LH,

RQS nº 03/2005 - CN
CPMI - CORREIOS
0751
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.113
CA.

1000BASE-ZX, 1000BASE-T, and coarse-wave division multiplexing (CWDM) GBICs. The dual GBIC-based Gigabit Ethernet implementation provides customers with tremendous deployment flexibility—allowing customers increased availability with the redundant uplinks. In sum, the configuration permits customers to implement one type of stacking and uplink configuration today, while preserving the option to migrate to another configuration in the future. High levels of stack resiliency can also be implemented by deploying dual-redundant Gigabit Ethernet uplinks, a redundant GigaStack GBIC loopback cable, Cisco UplinkFast and CrossStack UplinkFast technologies for high-speed uplink and stack interconnection failover, and Per-VLAN Spanning Tree Plus (PVST+) for uplink load balancing.

The Cisco Catalyst 2950T-24 Switch offers small and medium-sized enterprises server connectivity and an easy migration path to Gigabit by using the existing copper cabling infrastructure. Implementing Gigabit Ethernet over copper allows network managers to boost network performance and maximize infrastructure investments in Category 5 copper cabling.

Maximum power availability for a converged voice and data network is attainable when a Cisco Catalyst 2950 Series Switch is combined with the Cisco Redundant Power System (RPS) 300 or RPS 675 for protection against internal power supply failures and an uninterruptable power supply (UPS) system to safeguard against power outages.

Other Cisco Catalyst 2950 Series Switches

Cisco Catalyst 2950 Series with Cisco SI Software

The Cisco Catalyst 2950SX-24, 2950-24, and 2950-12 switches are also members of the Cisco Catalyst 2950 Series. They are standalone, fixed-configuration, and managed 10/100 switches providing basic workgroup connectivity for small to medium-sized companies. These wire-speed desktop switches come with Cisco SI Software features and offer Cisco IOS Software functioning for basic data, video, and voice services at the edge of the network.

Cisco Catalyst 2950 Series Long-Reach Ethernet Switches

- *Cisco Catalyst 2950ST-24-LRE*—24 long-reach Ethernet (LRE) ports, 2 fixed 10/100/1000BASE-T ports, and two small form factor pluggable (SFP) ports (2 of the 4 uplinks active at one time)
- *Cisco Catalyst 2950ST-8-LRE*—Eight LRE ports, 2 fixed 10/100/1000BASE-T ports, and two SFP ports (two of the four uplinks active at one time)

The Cisco Catalyst 2950 Series LRE switch solution delivers cost-effective, high-performance broadband access over existing phone wiring in enterprise campus environments and multitenant buildings (hotels, apartment buildings, and office buildings, for example). Cisco Catalyst 2950 Series LRE switches come with Cisco EI Software features, enabling enterprise and service provider customers to extend intelligent services over legacy wiring (Category 1, 2, and 3) to distances up to 5000 feet. Cisco is the only company with technologies that allow customers to deliver intelligent network services across any combination of wired and wireless infrastructures. Refer to the Cisco Catalyst 2950 Series LRE Data Sheet for more information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0752
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-112
4.

Intelligence in the Network

Networks are evolving to address four new developments at the network edge:

- Increase in desktop computing power
- Introduction of bandwidth-intensive applications
- Expansion of highly sensitive data on the network
- Presence of multiple device types, such as IP phones and wireless LAN (WLAN) access points

These new demands are contending for resources with many existing mission-critical applications. As a result, IT professionals must view the edge of the network as critical to the effective management of the delivery of information and applications.

As companies increasingly rely on networks as the strategic business infrastructure, it is more important than ever to ensure high availability, security, scalability, and control. By adding Cisco intelligent functioning to the wiring closet, customers can now deploy network-wide intelligent services that address these requirements in a consistent way, from the desktop to the core and through the WAN.

With Cisco Catalyst switches, Cisco enables companies to fully realize the benefits of adding intelligent services into their networks. Making the network infrastructure highly available to accommodate time-critical needs, scalable to accommodate growth, secure enough to protect confidential information, and capable of differentiating and controlling traffic flows is critical to further optimizing network operations.

Network Security Through Advanced Security Features

Cisco Catalyst 2950 Series switches offer enhanced data security through numerous security features. These features allow customers to enhance LAN security with capabilities to secure network management traffic through the protection of passwords and configuration information; to provide options for network security based on users, ports, and Media Access Control (MAC) addresses; and to enable more immediate reactions to intruder and hacker detection. These security enhancements are available free of charge by downloading the latest software release for the Cisco Catalyst 3550 and 2950 series switches.

Secure Shell (SSH) and SNMPv3 protect information from tampering or eavesdropping by encrypting information being passed along the network, guarding administrative information. Private VLAN Edge isolates ports on a switch, ensuring that traffic travels directly from the entry point to the aggregation device through a virtual path and that it cannot be directed to another port. Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.

Port-based access control parameters (ACPs) restrict sensitive portions of the network by denying packets based on source and destination MAC addresses, IP addresses, or Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports. ACP lookups are performed in hardware; therefore, forwarding performance is not compromised when implementing this type of security in the network. In addition, time-based access control lists (ACLs) allow configuration of differentiated services based on time periods. ACLs can also be applied to filter traffic based on Differentiated Services Code Point (DSCP) values. Port security provides another means to ensure the appropriate user is on the network by limiting access based on MAC addresses.

For authentication of users with a Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) server, 802.1x provides port-level security. In conjunction with a RADIUS server, 802.1x allows for dynamic port-based user authentication, which can be extended to dynamically

RQS nº 03/2005 - CN
CPMI - CORREIOS
0753
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

assign a virtual LAN (VLAN) based on a specific user, regardless of where they connect on the network. This intelligent adaptability allows IT departments to offer greater flexibility and mobility to their stratified user populations. By combining access control and user profiles with secure network connectivity, services, and applications, enterprises can more effectively manage user mobility and drastically reduce the overhead associated with granting and managing access to network resources.

With multilayer Cisco Catalyst 2950 Series switches, network managers can implement high levels of console security. Multilevel access security on the switch console and the Web-based management interface prevent unauthorized users from accessing or altering switch configuration. TACACS+ or RADIUS authentication enables centralized access control of the switch and restricts unauthorized users from altering the configuration. Deploying security can be done through Cisco CMS Software security wizards, which ease the deployment of security features that restrict user access to a server, a portion of the network, or the entire network.

Network Control Through Advanced QoS and Rate Limiting

Cisco Catalyst 2950 Series switches offer superior and highly granular QoS based on Layer 2–4 information to ensure that network traffic is classified and prioritized, and that congestion is avoided in the best possible manner. Configuration of QoS is greatly simplified through automatic QoS (auto-QoS), a feature that detects Cisco IP phones and automatically configures switches for the appropriate classification and egress queuing. This optimizes traffic prioritization and network availability without the challenge of a complex configuration.

Cisco Catalyst 2950 Series switches can classify, reclassify, police (determine if the packet is in or out of predetermined profiles and affect actions on the packet), and mark or drop the incoming packets before the packet is placed in the shared buffer. Packet classification allows the network elements to discriminate between various traffic flows and enforce policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, these switches first identify traffic flows (or packet groups) and classify or reclassify these groups using the DSCP field in the IP packet or the 802.1p class of service (CoS) field in the Ethernet packet. Classification and reclassification can also be based on criteria as specific as the source/destination IP address, source/destination MAC address, or the Layer 4 TCP/UDP ports. At the ingress (incoming port) level, the Cisco Catalyst switches will also perform policing and marking of the packet.

After the packet goes through classification, policing, and marking, it is assigned to the appropriate queue before exiting the switch. Cisco Catalyst 2950 Series switches support four egress (outgoing port) queues per port, which allows the network administrator to be more discriminating and specific in assigning priorities for the various applications on the LAN. At the egress level, the switch performs scheduling, which is a process that determines the order in which the queues are processed. The switches support Weighted Round Robin (WRR) scheduling or strict priority scheduling. The WRR scheduling algorithm ensures that lower priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority scheduling ensures that the highest priority packets will always get serviced first, ahead of all other traffic, and that the other three queues will be serviced using WRR best effort.

These features allow network administrators to ptioritize mission-critical or bandwidth-intensive traffic, such as enterprise resource planning (ERP) (Oracle, SAP, and so on), voice (IP telephony traffic), and CAD/CAM over less time-sensitive applications such as File Transfer Protocol (FTP) or e-mail (SMTP). For example, it would be highly undesirable to have a large file download destined to one port on a wiring closet switch and have quality implications,

RQS nº 03/2005 - CN
CPMI - CORREIOS
0754
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

such as increased latency in voice traffic, destined to another port on this switch. This condition is avoided by ensuring that voice traffic is properly classified and prioritized throughout the network. Other applications, such as Web browsing, can be treated as low priority and handled on a best-effort basis.

Cisco Catalyst 2950 Series switches are capable of allocating bandwidth based on several criteria, including MAC source address, MAC destination address, IP source address, IP destination address, and TCP/UDP port number. Bandwidth allocation is essential in network environments that require service-level agreements, or when it is necessary for the network manager to control the bandwidth given to certain users. Cisco Catalyst 2950 Series switches support up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port, giving the network administrator granular control of LAN bandwidth.

Network Availability

To provide efficient use of resources for bandwidth-hungry applications like multicasts, Cisco Catalyst 2950 Series switches support Internet Group Management Protocol (IGMP) snooping in hardware. Through the support and configuration of IGMP snooping via Cisco CMS Software, Cisco Catalyst 2950 Series switches deliver outstanding performance and ease of use in administering and managing multicast applications on the LAN.

The IGMP snooping feature allows the switch to "listen in on" the IGMP conversation between hosts and routers. When a switch hears an "IGMP join" request from a host for a given multicast group, the switch adds the host's port number to the group destination address (GDA) list for that group. When the switch hears an "IGMP leave" request, it removes the host's port from the content-addressable memory (CAM) table entry.

PVST+ allows users to implement redundant uplinks while distributing traffic loads across multiple links. This is not possible with standard Spanning-Tree Protocol implementations. Cisco UplinkFast technology helps ensure immediate transfer to the secondary uplink, an improvement over the traditional 30-to-60 second convergence time. An additional feature that enhances performance is Voice VLAN, which allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony—simplifying phone installations and providing easier network traffic administration and troubleshooting.

Multicast VLAN Registration (MVR) is designed for applications that use wide-scale deployment of multicast traffic across an Ethernet-ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN.

Network Management

Cisco CMS Software is Web-based and embedded in Cisco Catalyst 3550, 2950, 3500 XL, 2900 XL, and 2900 LRE XL series switches. Through Cisco switch clustering technology, users can access Cisco CMS Software with any standard Web browser to manage up to 16 of these switches at once, regardless of their geographic proximity—with the option of using a single IP address for the entire cluster if desired. With the addition of the Cisco Catalyst 3550 Series switches, Cisco CMS Software can now extend beyond routed boundaries for even more flexibility in managing a Cisco cluster.

Cisco CMS Software provides an integrated management interface for delivering intelligent services, such as multilayer switching, QoS, multicast, and security ACLs. Cisco CMS Software allows administrators to take advantage of benefits formerly reserved for only the most advanced networks without having to learn the command-line interface (CLI) or even the details of the technology.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0755
Doc. 3690

15.109
CA.

The new Guide Mode in Cisco CMS Software leads the user step-by-step through the configuration of advanced features and provides enhanced online help for context-sensitive assistance. In addition, Cisco AVVID (Architecture for Voice, Video and Integrated Data) wizards provide automated configuration of the switch to optimally support video streaming or videoconferencing, voice over IP (VoIP), and mission-critical applications. These wizards can save hours of time for network administrators, eliminate human errors, and help ensure that the configuration of the switch is optimized for these applications.

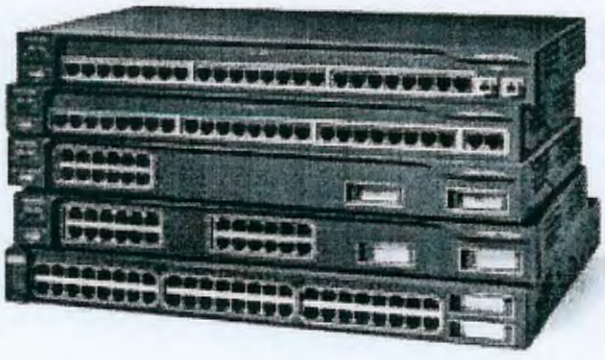
Cisco CMS Software supports standards-based connectivity options such as Ethernet, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet, and Gigabit EtherChannel connectivity. Because Cisco switch clustering technology is not limited to a single stack of switches, Cisco CMS Software expands the traditional cluster domain beyond a single wiring closet and saves time and effort for network administrators.

Cisco Catalyst 2950 Series switches can be configured either as command or member switches in a Cisco switch cluster. Cisco CMS Software also allows the network administrator to designate a standby or redundant command switch, which takes the commander duties should the primary command switch fail. Other features include the ability to configure multiple ports and switches simultaneously, to perform software updates across the entire cluster at once, and to clone configurations to other clustered switches for rapid network deployment. Bandwidth graphs and link reports provide useful diagnostic information, and the topology map gives network administrators a quick view of the network status.

In addition to Cisco CMS Software, Cisco Catalyst 2950 Series switches provide extensive management tools using SNMP network management platforms such as CiscoWorks for switched internetworks.

Cisco Catalyst 2950 Series switches deliver a comprehensive set of management tools to provide the required visibility and control in the network (Figure 1). Managed with CiscoWorks, Cisco Catalyst switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Figure 1
Cisco Catalyst 2950 Series Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0756
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.108

Product Features and Benefits

Table 1 lists the features and benefits of the Cisco Catalyst 2950 Series switches.

Table 1 Features and Benefits

Feature	Benefit
Availability	
Superior redundancy for fault backup	• IEEE 802.1D Spanning-Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • Support for Cisco Spanning-Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies ensure quick failover recovery, enhancing overall network stability and availability. • IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) provides rapid convergence of the spanning tree independent of spanning-tree timers. • Cisco CrossStack UplinkFast technology extends UplinkFast to a stack to ensure quick failover recovery, enhancing network stability and availability. • Support for the optional 300-watt or 675-watt redundant Cisco AC power system provides a backup power source for up to 4 or 6 units, respectively, for improved fault tolerance and network uptime. • Redundant stacking connections provide support for a redundant loopback connection for top and bottom switches in an independent stack backplane cascaded configuration. • Command switch redundancy enabled in Cisco CMS Software allows customers to designate a backup command switch that takes over cluster management functions if the primary command switch fails. • Unidirectional link detection (UDLD) and aggressive UDLD features detect and disable unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Software features for bandwidth optimization	• Bandwidth aggregation of up to 4 Gbps (2 ports full duplex) through Cisco Gigabit EtherChannel® technology and up to 16 Gbps (8 ports full duplex) through Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches, to routers and individual servers. Port Aggregation Protocol (PAgP) is available to simplify configuration. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) allows a spanning tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • IGMP snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. MVR, IGMP filtering, fast-join, and immediate leave are available as enhancements. • MVR continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons. • Supports additional frame formats: Ethernet II (tagged and untagged), 802.3 (sequence number protection [SNAP] encapsulated tagged and untagged frames)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0757
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Feature	Benefit
Security	
Network-wide security features	• Filtering of incoming traffic flows based on Layer 2–4 ACPs prevents unauthorized data flows. – The following Layer 2 ACPs (or a combination) can be used for security classification of incoming packets: source MAC address, destination MAC address, and 16-bit Ethertype. – The following Layer 3 and Layer 4 fields (or a combination) can be used for security classification of incoming packets: source IP address, destination IP address, TCP source or destination port number, UDP source, or destination port number. ACLs can also be applied to filter based on DSCP values. – Time-based ACLs allow configuration of differentiated services based on time periods. • A private VLAN edge provides security and isolation between ports on a switch, helping to ensure that voice traffic travels directly from its entry point to the aggregation device through a virtual path and that it cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated, regardless of which LAN port they are accessing, and provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. . 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user, regardless of where the user is connected. . 802.1x with an ACL assignment allows for specific security policies based on a user, regardless of where the user is connected. . 802.1x with Voice VLAN gives an IP phone access to the Voice VLAN regardless of the authorized or unauthorized state of the port. • 802.1x with port security enables authenticating the port and managing network access for all MAC addresses, including that of the client. • SSH and SNMPv3 provides network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH and the crypto version of SNMPv3 require a special crypto software image due to U.S. export restrictions. • Port Security secures the access to a port based on the MAC address of a user's device. The aging feature removes the MAC address from the switch after a specific timeframe to allow another device to connect to the same port. • MAC Address Notification allows administrators to be notified of new users added or removed from the network. • Spanning-tree root guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning-Tree Protocol root nodes. • The Spanning-Tree Protocol PortFast/bridge protocol data unit (BPDU) guard feature disables access ports with Spanning-Tree Protocol PortFast-enabled upon reception of a BPDU, and increases network reliability, manageability, and security. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • The user-selectable address-learning mode simplifies configuration and enhances security. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and to disable the trust setting in the event that the IP phone is removed, preventing a rogue user from overriding prioritization policies in the network. • IGMP Filtering provides multicast authentication by filtering out nonsubscribers and limiting the number of concurrent multicast streams available per port. • Support for dynamic VLAN assignment through implementation of the VLAN Membership Policy Server (VMPS) client function provides flexibility in assigning ports to VLANs. Dynamic VLAN enables fast assignment of IP addresses. • Cisco CMS Software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or the entire network.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0758
Doc. 3690

Feature	Benefit
QoS	
Overview	• The switches support the aggregate QoS model by enabling classification, policing/metering, and marking functions on a per-port basis at ingress and the queuing/scheduling function at egress. • The switches support configuring QoS ACPs on all ports to ensure proper policing and marking on a per-packet basis using ACPs. Up to 4 ACPs per switch are supported in configuring either QoS ACPs or security filters. • Auto-QoS greatly simplifies the configuration of QoS in VoIP networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration.
Qos classification support at ingress	• The switches support QoS classification of incoming packets for QoS flows based on Layer 2–4 fields. • The following Layer 2 fields (or a combination) can be used for classifying incoming packets to define QoS flows: source MAC address, destination MAC address, and 16-bit Ethertype. • The switches support identification of traffic based on Layer 3 type of service (ToS) field and DSCP values. • The following Layer 3 and 4 fields (or a combination) can be used to classify incoming packets to define QoS flows: source IP address, destination IP address, TCP source or destination port number, and UDP source or destination port number.
Qos metering/policing at ingress	• Support for metering/policing of incoming packets restricts incoming traffic flows to a certain rate. • The switches support up to 6 policers per Fast Ethernet port, and 60 policers on a Gigabit Ethernet port. • The switches offer granularity of traffic flows at 1 Mbps on Fast Ethernet ports, and 8 Mbps on Gigabit Ethernet ports.
Qos marking at ingress	• The switches support marking/remarking packets based on state of policers/meters. • The switches support marking/remarking based on the following mappings: from DSCP to 802.1p, and from 802.1p to DSCP. • The switches support 14 widely used DSCP values. • The switches support classifying or reclassifying packets based on default DSCP per port. They also support classification based on DSCP values in the ACL. • The switches support classifying or reclassifying frames based on the default 802.1p value per port. • The switches support 802.1p override at ingress.
QoS scheduling support at egress	• 4 queues per egress port are supported in hardware. • The WRR queuing algorithm ensures that low-priority queues are not starved. • Strict-priority queue configuration via Strict Priority Scheduling ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Sophisticated traffic management	• The switch supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. • The switch offers granularity of traffic flows at 1 Mbps on Fast Ethernet ports and 8 Mbps on Gigabit Ethernet ports. • The switch offers the ability to limit data flows based on MAC source/destination address, IP source/destination address, TCP/UDP port numbers, or any combination of these fields. • The switch offers the ability to manage data flows asynchronously upstream and downstream from the end station or on the uplink.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0259
Fls. Nº
Doc. 3690

15.105
4.

Feature	Benefit
Management	
Superior manageability	• An embedded Remote Monitoring (RMON) software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • The switch supports all 9 RMON groups through the use of a Cisco SwitchProbe® Analyzer (Switched Port Analyzer [SPAN]) port, permitting traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe. • A SPAN port monitors traffic of a single port from a single network analyzer or RMON probe. • Remote Switch Port Analyzer (RSPAN) allows network administrators to locally monitor ports in a Layer 2 switch network from any other switch in the same network. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 Traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Crash Information Support enables a switch to generate a crash file for improved troubleshooting. • Show-interface-capabilities provides information on configuration capabilities of any interface. • The RTTMON Management Information Base (MIB) allows users to monitor network performance between a Cisco Catalyst switch and a remote device. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BASE-T/100BASE-TX/1000BASE-T indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization, provide a comprehensive and convenient visual management system.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0760
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.104
A.

Feature	Benefit
Management	
Cisco CMS Software	• Cisco CMS Software allows the user to manage up to 16 interconnected Cisco Catalyst 3550, 2950, 3500 XL, 2900 XL, and 2900 LRE XL series switches without the limitation of being physically located in the same wiring closet, and with the option of using a single IP address for the entire cluster if desired. Full backward compatibility helps ensure that any combination of the above switches can be managed with a Cisco Catalyst 2950 Series switch. • Cisco AVVID wizards use just a few user inputs to automatically configure the switch to optimally handle different types of traffic—voice, video, multicast, or high-priority data. • A security wizard is provided to restrict unauthorized access to servers and networks, and to restrict certain applications on the network. • One-click software upgrades can be performed across the entire cluster simultaneously, and configuration cloning enables rapid deployment of networks. • Cisco CMS Software has been extended to include multilayer feature configurations such as ACPs and QoS parameters. • Cisco CMS Software Guide Mode assists users in the configuration of powerful advanced features by providing step-by-step instructions. • Cisco CMS Software provides enhanced online help for context-sensitive assistance. • An easy-to-use graphical interface provides both a topology map and a front-panel view of the cluster. • Multidevice and multiport configuration capabilities allow network administrators to save time by configuring features across multiple switches and ports simultaneously. • Ability to launch the Web-based management for a Cisco Aironet® Wireless Access Point by simply clicking on its icon in the topology map. • A user-personalized interface allows users to modify polling intervals, table views, and other settings within Cisco CMS Software and to retain these settings the next time they use the software. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Support for CiscoWorks	• Manageable through CiscoWorks network management software on a per-port and per-switch basis provides a common management interface for Cisco routers, switches, and hubs. • SNMP v1, v2, and v3 (non-crypto) and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Cisco Discovery Protocol Versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Supported by the CiscoWorks LAN Management Solution.

RQS nº 03/2005 - CN
CPMI— — CORREIOS
Fls. Nº 0761
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.103
CA.

Feature	Benefit
Management	
Ease of use and ease of deployment	• The Cisco GigaStack® GBIC delivers a hardware-based, independent stacking bus with up to a 2-Gbps forwarding rate in a point-to-point configuration, or 1 Gbps of forwarding bandwidth when daisy-chained with up to 9 switches. • Autoconfiguration eases the deployment of switches in the network by automatically configuring multiple switches across a network via a boot server. • Auto-QoS greatly simplifies the configuration of QoS in VoIP networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration. • Autosensing on each non-GBIC port detects the speed of the attached device and automatically configures the port for 10-, 100-, or 1000-Mbps operation, easing the deployment of the switch in mixed 10, 100, and 1000BASE-T environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • DTP enables dynamic trunk configuration across all ports in a switch. • PAgP automates the creation of Cisco Fast EtherChannel or Gigabit EtherChannel groups, enabling linking to another switch, router, or server. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This is similar to Cisco EtherChannel and PAgP. • IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, and 1000BASE-T physical interface support through a field-replaceable GBIC module provides customers unprecedented flexibility in switch deployment. • The default configuration stored in Flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention. • The switches support nonstandard Ethernet frame sizes (mini-giants) up to 1542 bytes (configurations with GBIC ports only).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 762
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15-10-2
A-

Product Specifications

Feature	Description
Performance	• 13.6-Gbps switching fabric • Cisco Catalyst 2950G-48: 13.6 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-24: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-24-DC: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-12: 6.4 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950T-24: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950C-24: 5.2 Gbps maximum forwarding bandwidth (Forwarding rates based on 64-byte packets) • Cisco Catalyst 2950G-48: 10.1-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24-DC: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-12: 4.8-Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950C-24: 3.9-Mpps wire-speed forwarding rate • 8 MB memory architecture shared by all ports • Up to 16 MB SDRAM and 8 MB Flash memory • Configurable up to 8000 MAC addresses • Configurable maximum transmission unit (MTU) of up to 1530 bytes (Cisco Catalyst 2950G switches only)
Management	• BRIDGE-MIB • CISCO-BULK-FILE-MIB • CISCO-2900-MIB • CISCO-CDP-MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-IMAGE-MIB • CISCO-IPMROUTE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-SMI • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TC • CISCO-TCP-MIB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0763
3690
Doc.

Feature	Description
Management	• CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.1w • IEEE 802.1s • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning-Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3ad • IEEE 802.3z 1000BASE-X specification • 1000BASE-X (GBIC) • 1000BASE-T (GBIC) • 1000BASE-SX • 1000BASE-LX/LH • 1000BASE-ZX • 1000BASE-CWDM GBIC 1470 nm • 1000BASE-CWDM GBIC 1490 nm • 1000BASE-CWDM GBIC 1510 nm • 1000BASE-CWDM GBIC 1530 nm • 1000BASE-CWDM GBIC 1550 nm • 1000BASE-CWDM GBIC 1570 nm • 1000BASE-CWDM GBIC 1590 nm • 1000BASE-CWDM GBIC 1610 nm

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0764
Doc. 3690

15.100
JA.

Feature	Description
Standards	• RMON I and II standards • SNMPv1, v2c, and v3 (planned future support for v3)
Y2K	• Y2K compliant
Connectors and cabling	• 10BASE-T ports: RJ-45 connectors; two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BASE-TX ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 1000BASE-T ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 100BASE-FX ports: MT-RJ connectors, 50/125 or 62.5/125 micron multimode fiber-optic cabling • 1000BASE-T, 1000BASE-SX, -LX/LH, -ZX GBIC-based ports: SC fiber connectors, single-mode or multimode fiber • Cisco GigaStack GBIC ports: copper-based Cisco GigaStack cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-RJ-45 rollover cable with RJ-45-to-DB9 adapter for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately from Cisco, part number ACS-DSBUASYN=)
MT-RJ patch cables for Cisco Catalyst 2950C-24 Switch	*Type of cable, Cisco part number* • 1-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-1M • 3-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-3M • 5-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-5M • 1-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-1M • 3-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-3M • 5-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-5M
Power connectors	Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 300. The connectors are located at the back of the switch. **Internal power supply connector** • The internal power supply is an autoranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • The supplied AC power cord should be used to connect the AC power connector to an AC power outlet. **Cisco RPS 675 Connector** • The connector offers connection for an optional Cisco RPS 675 that uses AC input and supplies DC output to the switch. • The connector offers a 675-watt redundant power system that can support six external network devices and provides power to one failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Attach only the Cisco RPS 675 (model PWR675-AC-RPS-NI=) to the RPS receptacle with this connector. **Cisco RPS 300 Connector** • The connector offers connection for an optional Cisco RPS 300 that uses AC input and supplies DC output to the switch. • The connector offers a 300-watt redundant power system that can support six external network devices and provides power to one failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle with this connector.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0765
Doc. 3690

15.099
4-

Feature	Description
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications. • System status LEDs: system, RPS, and bandwidth utilization indications.
Dimensions (H x W x D) and weight	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.5 x 24.18 cm) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • 1.72 x 17.5 x 13 in. (4.36 x 44.5 x 33.02 cm) (Cisco Catalyst 2950G-48) • 1.0 rack-unit (RU) high • 6.5 lb (3.0 kg) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • 10 lb (4.5 kg) (Cisco Catalyst 2950G-48)
Environmental ranges	• Operating temperature: 32 to 113°F (0° to 45°C) • Storage temperature: –13° to 158°F (–25° to 70°C) • Operating relative humidity: 10 to 85 percent (noncondensing) • Operating altitude: Up to 10,000 ft (3000 m) • Storage altitude: Up to 15,000 ft (4500 m) • Not intended for use on top of desktops or in open office environments
Power requirements	• Power consumption: 30W maximum, 102 BTUs per hour (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • Power consumption: 45W maximum, 154 BTUs per hour (Cisco Catalyst 2950G-48) • AC input voltage/frequency: 100 to 127/200 to 240 VAC (autoranging); 50 to 60 Hz • DC input voltages for Cisco RPS 300: +12V @ 4.5A
Acoustic noise	• ISO 7770, bystander position—operating to an ambient temperature of 30°C: – WS-C2950-24, WS-C2950-12, WS-C2950C-24, WS-C2950T-24: 46 dBa – WS-C2950G-12, WS-C2950G-24: 46 dBa – WS-C2950G-48: 48 dBa
Predicted mean time between failure (MTBF)	• 482,776 hours (Cisco Catalyst 2950G-12) • 468,884 hours (Cisco Catalyst 2950G-24) • 479,086 hours (Cisco Catalyst 2950G-24-DC) • 159,026 hours (Cisco Catalyst 2950G-48) • 297,144 hours (Cisco Catalyst 2950T-24) • 268,292 hours (Cisco Catalyst 2950C-24)
Fiber-port specifications for Cisco Catalyst 2950C-24 Switch	Fiber-port power levels: • Optical transmitter wavelength: 1300 nm • Optical receiver sensibility: –14 dBm2 • Optical transmitter power: –19 to –14 dBm • Transmit: –19 to –14 dBm

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0766
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

15.098
JA.

Feature	Description
Regulatory Agency Approvals	
Safety certifications	• UL 1950/CSA 22.2 No. 950 • IEC 950-EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic emissions certifications	• FCC Part 15 Class A • EN 55022: 1998 Class A (CISPR22 Class A) • EN 55024: 1998 (CISPR24) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 • BSMI Class A • MIC
Network Equipment Building Standards (NEBS) (For WS-C2950G-24-EI-DC only)	• Bellcore • GR-1089-CORE • GR-63-CORE • SR-3580 Level 3
Warranty	• Limited lifetime warranty

Service and Support

The services and support programs described in Table 2 are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers.

Table 2 Service and Support Programs

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)—available direct from Cisco ***Packaged TIS***—available through resellers	• Project management • Site survey and configuration deployment • Installation, text, and cutover • Training • Major moves, adds, and changes • Design review and product staging	• Supplements existing staff • Ensures that functions meet customer needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet® and Cisco SMARTnet Onsite services—available direct from Cisco ***Packaged Cisco SMARTnet service***—available through resellers	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Cisco Technical Assistance Center (TAC) • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by using Cisco expertise and knowledge • Minimizes network downtime

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0767
Doc. 3690

Ordering Information

Model Numbers	Configuration
WS-C2950G-48-EI	• 48 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950G-24-EI	• 24 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950G-24-EI-DC	• 24 10/100 ports and 2 1000BASE-X ports; DC power • Cisco EI Software image installed
WS-C2950G-12-EI	• 12 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950T-24	• 24 10/100 ports and 2 1000BASE-T ports • Cisco EI Software image installed
WS-C2950C-24	• 24 10/100 ports and 2 100BASE-FX ports • Cisco EI Software image installed
WS-C2950ST-24-LRE	• 24 LRE ports, 2 fixed 10/100/1000BASE-T ports, and 2 SFP ports • Cisco EI Software image installed
WS-C2950ST-8-LRE	• 8 LRE ports, 2 fixed 10/100/1000BASE-T ports, and 2 SFP ports • Cisco EI Software image installed

For More Information

- United States and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- http://www.cisco.com

15.097 JA

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, GigaStack, SwitchProbe are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

BCDL-W4574 05/03

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0768
Fls. Nº
3690
Doc.

roriz@IBM-297NYWD11S3

15.096
LA-

Job Title: SWITCH_TIPO2_doc2.pdf

Time Queued: Thu Jul 24 03:30:31 2003
Time Printed: Thu Jul 24 04:03:44 2003

Submitted By: roriz@IBM-297NYWD11S3

Need help? Call your local NCO HelpDesk.

PIO_DEV: ibm@brbrap7a#ibmNetPrinter (ibm4320) @ brbraprt01

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0769
Doc. 3690

roriz@IBM-297NYWD11S3

15.095
-4-

Overview

This chapter provides information about these topics:

- Switch features
- Front- and rear-panel descriptions
- Management options

Features

The Catalyst 2950 switches are stackable Ethernet switches to which you can connect workstations and other network devices, such as servers, routers, and other switches. The switches can be deployed as backbone switches, aggregating 10BASE-T, 100BASE-TX, and Gigabit Ethernet traffic from other network devices. Refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* for examples showing how you might deploy the switches in your network.

Table 1-1 lists the switch features, and Figure 1-1 through Figure 1-8 show the Catalyst 2950 switches.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0770
Doc. 3690

15.094
VA

Table 1-1 Catalyst 2950 Switch Features

Feature	Description
Hardware	• Catalyst 2950-12 switch—12 10/100 Ethernet ports • Catalyst 2950-24 switch—24 10/100 Ethernet ports • Catalyst 2950C-24 switch—24 10/100 Ethernet ports and 2 100BASE-FX ports • Catalyst 2950G-12-EI—12 10/100 Ethernet ports and 2 GBIC[1]-based Gigabit Ethernet module slots • Catalyst 2950G-24-EI—24 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet module slots • Catalyst 2950G-24-EI-DC[2]—24 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet module slots with DC-input power • Catalyst 2950G-48-EI—48 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet module slots • Catalyst 2950T-24 switch—24 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports • On Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, and 2950G-48-EI switches, support for these GBIC modules: – 1000BASE-SX GBIC – 1000BASE-LX/LH GBIC – 1000BASE-ZX GBIC – GigaStack GBIC

RQS nº 03/2005 - CN
CPMI--- CORREIOS
Fls. Nº 0771
Doc. 3690

15.093
A.

Table 1-1 Catalyst 2950 Switch Features (continued)

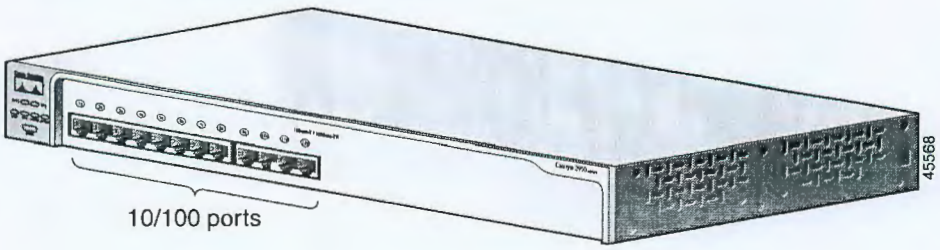
Feature	Description
Configuration	• Autonegotiates the speed and duplex settings on 10/100 ports and on 10/100/1000 ports • Supports only 100-Mbps and full-duplex settings on 100BASE-FX ports • Supports 8192 MAC addresses • Checks for errors on a received packet, determines the destination port, stores the packet in shared memory, and then forwards the packet to the destination port
Power redundancy	• Connection for an optional Cisco RPS 300 Redundant Power System (RPS) that uses AC[3] input and supplies DC output to the switch

1. GBIC = Gigabit Interface Converter
2. DC = direct current
3. AC = alternating current

Front-Panel Description

The switch front panel contains the ports, the LEDs, and the Mode button. Figure 1-1 to Figure 1-8 show the switches.

Figure 1-1 Catalyst 2950-12 Switch



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0772
Doc. 3690

Figure 1-2 Catalyst 2950-24 Switch

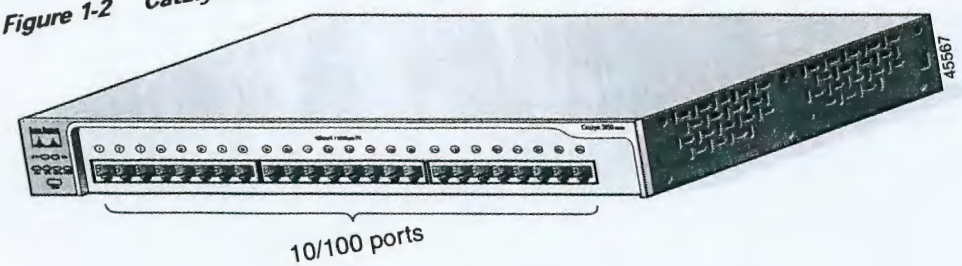


Figure 1-3 Catalyst 2950C-24 Switch

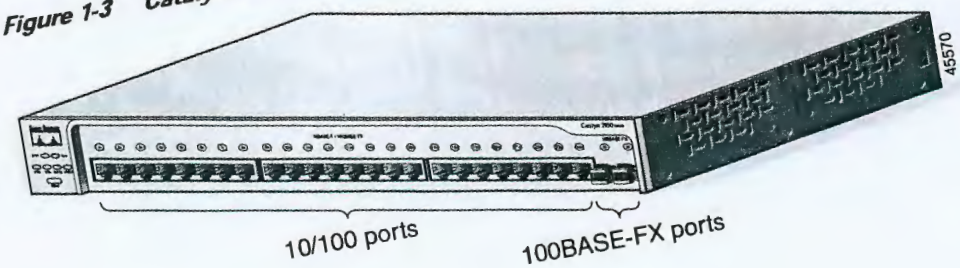
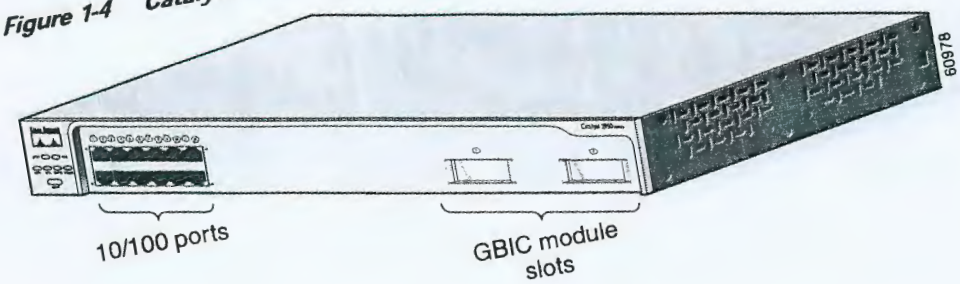


Figure 1-4 Catalyst 2950G-12-EI Switch



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0773
Doc. 3690

Figure 1-5 Catalyst 2950G-24-EI Switch

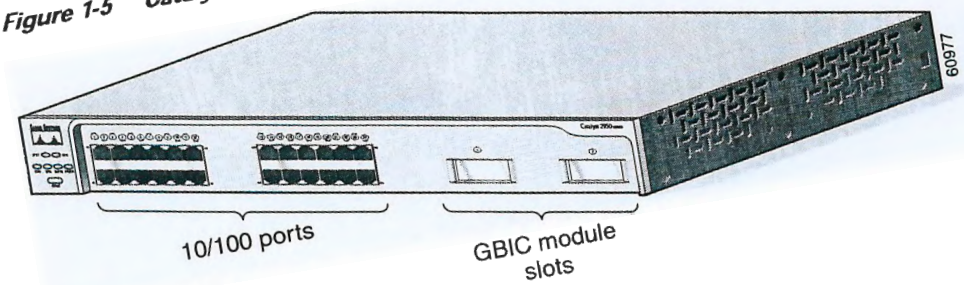


Figure 1-6 Catalyst 2950G-24-EI-DC Switch

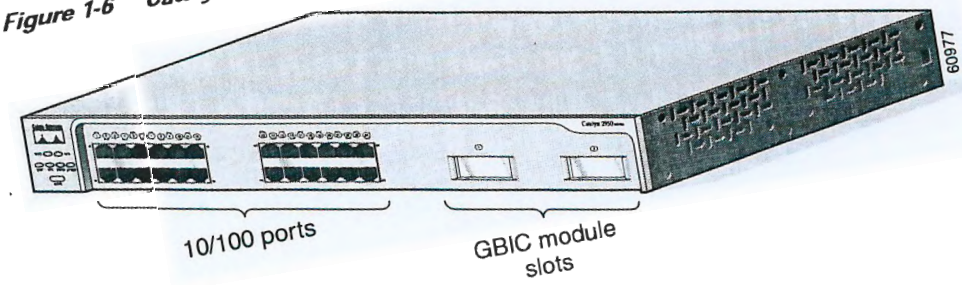
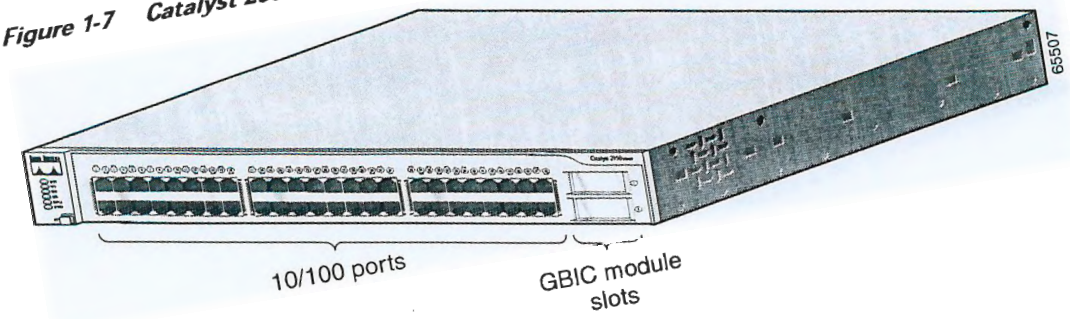


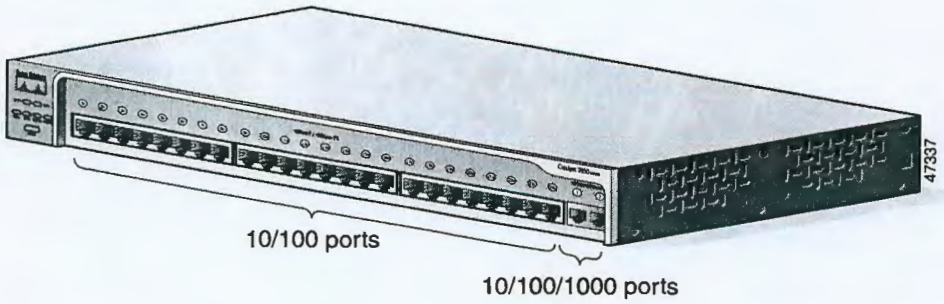
Figure 1-7 Catalyst 2950G-48-EI Switch



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0374
Doc: 3690

15.090
4

Figure 1-8 Catalyst 2950T-24 Switch



10/100 Ports

The 10/100 ports use RJ-45 connectors and twisted-pair cabling. The ports can connect to these devices:

- 10BASE-T-compatible devices, such as workstations and hubs, through standard RJ-45 connectors and two twisted-pair cabling. You can use Category 3, 4, or 5 cabling.
- 100BASE-TX-compatible devices, such as high-speed workstations, servers, hubs, routers, and other switches, through standard RJ-45 connectors and two or four twisted-pair, Category 5 cabling.

Note When connecting the switch to workstations, servers, and routers, be sure that the cable is a twisted-pair straight-through cable. When connecting the switch to hubs or other switches, use a twisted-pair crossover cable. Pinouts for the cables are described in Appendix B, "Connectors and Cables."

The 10/100 ports can be explicitly set to operate in any combination of half duplex, full duplex, 10 Mbps, or 100 Mbps. They can also be set for speed and duplex autonegotiation, compliant with IEEE 802.3U. In all cases, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0775
Doc. 3690

15.089
A.

When set for autonegotiation, a port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the attached device supports autonegotiation, the port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission, if the attached device supports it) and configures itself accordingly.

100BASE-FX Ports

The 100BASE-FX ports use 50/125- or 62.5/125-micron multimode fiber-optic cabling. These ports only operate at 100 Mbps in full-duplex mode.

In full-duplex mode (the default), the cable length from a switch to an attached device cannot exceed 6562 feet (2 kilometers).

You can connect a 100BASE-FX port to an SC or ST port on a target device by using one of the MT-RJ fiber-optic patch cables listed in Table 1-2. Use the Cisco part numbers in Table 1-2 to order the patch cables that you need.

Table 1-2 MT-RJ Patch Cables for 100BASE-FX Connections

Type	Cisco Part Number
1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0776
Doc. 3690

15.088
A-

10/100/1000 Ports

The 10/100/1000 ports on Catalyst 2950T-24 switches use RJ-45 connectors and twisted-pair cabling. The ports can connect to these devices:

- 10BASE-T-compatible devices, such as workstations and hubs, through standard RJ-45 connectors and two or four twisted-pair, Category 5 cabling.
- 100BASE-TX-compatible devices, such as high-speed workstations, servers, hubs, routers, and other switches, through standard RJ-45 connectors and two or four twisted-pair, Category 5 cabling.
- 1000BASE-T-compatible devices, such as high-speed workstations, servers, hubs, routers, and other switches, through standard RJ-45 connectors and four twisted-pair, Category 5 cabling.

Note When connecting to a 1000BASE-T-compatible device, be sure to use a four twisted-pair, Category 5 cable.

Note When connecting the switch to workstations, servers, and routers, be sure that the cable is a twisted-pair straight-through cable. When connecting the switch to hubs or other switches, use a twisted-pair crossover cable. Pinouts for the cables are described in Appendix B, "Connectors and Cables."

The 10/100/1000 ports on Catalyst 2950T-24 switches can be explicitly set to operate at 10 or 100 Mbps in half- or full-duplex mode or at 1000 Mbps in full-duplex mode. The default duplex setting is full duplex. They can also be set for speed and duplex autonegotiation, compliant with IEEE 802.3AB. In all cases, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).

RQS nº 03/2005 - CN
CPMI - CORREIOS
0777
Fls. Nº
3690
Doc.

15.087
A

GBIC Module Ports

The GBIC module slots support these modules:

- 1000BASE-SX GBIC module for fiber-optic connections that cannot exceed 1804 feet (550 meters).
- 1000BASE-LX/LH GBIC module for fiber-optic connections that cannot exceed 32,810 feet (10 kilometers).
- 1000BASE-ZX GBIC module for fiber-optic connections that cannot exceed 328,100 feet (100 kilometers).
- GigaStack GBIC module for creating a 1-Gbps stack configuration of up to nine supported switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to nine half-duplex links (in a stack configuration) to other Gigabit Ethernet devices. Using the required Cisco proprietary signaling and cabling, the GigaStack GBIC-to-GigaStack GBIC connection cannot exceed 3 feet (1 meter).

For more information about these GBICs, refer to your GBIC documentation.

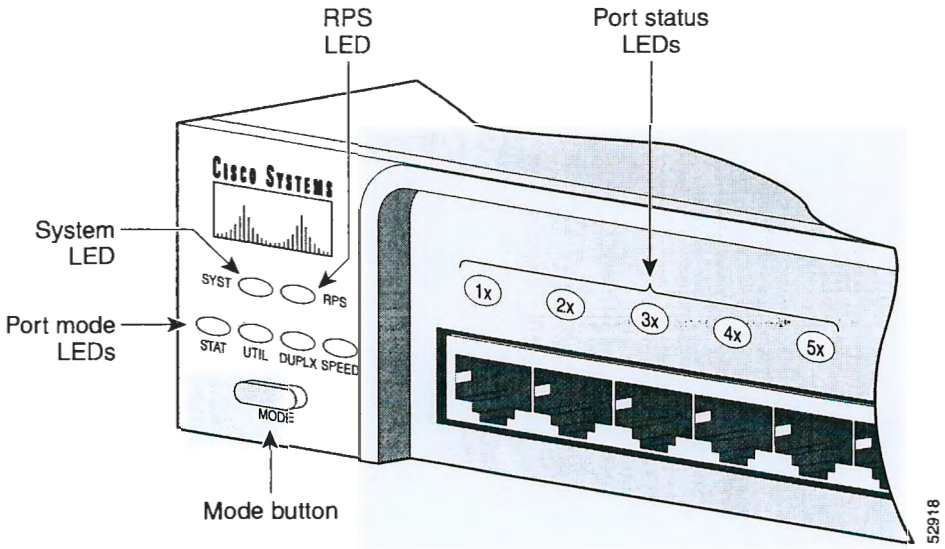
LEDs

You can use the LEDs to monitor switch activity and performance. Figure 1-9, Figure 1-10, and Figure 1-11 show the location of the LEDs and the Mode button that you use to select the port mode. Changing the port mode changes the information provided by each port status LED.

All of the LEDs described in this section except the utilization meter (UTIL) are visible in the Cluster Management Suite (CMS). The *Catalyst 2950 Desktop Switch Software Configuration Guide* describes how to use CMS to manage individual switches and switch clusters.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0778
3691
Doc.

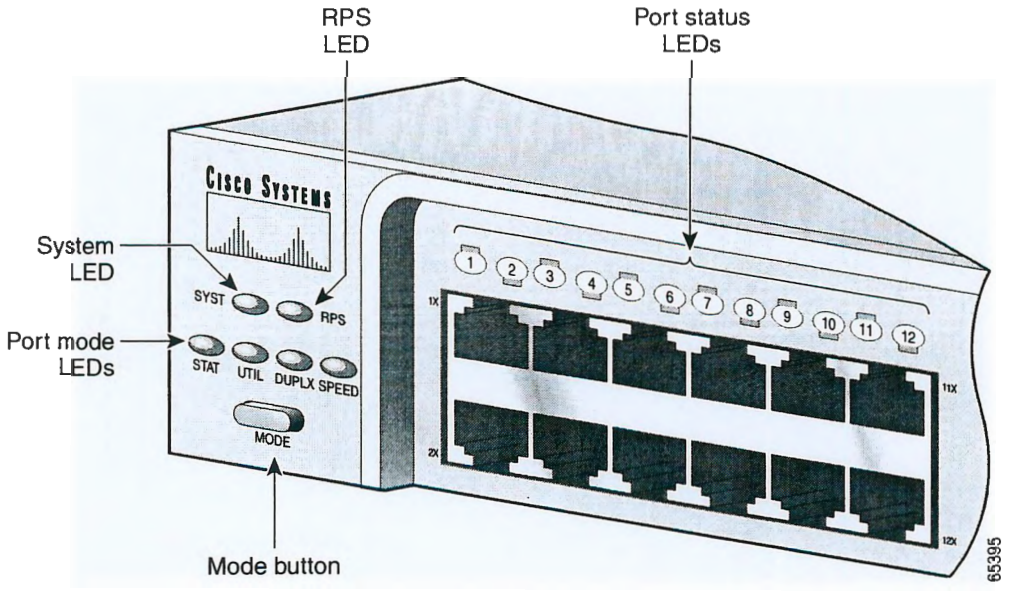
Figure 1-9 LEDs on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0779
Doc 3690

15.085
A

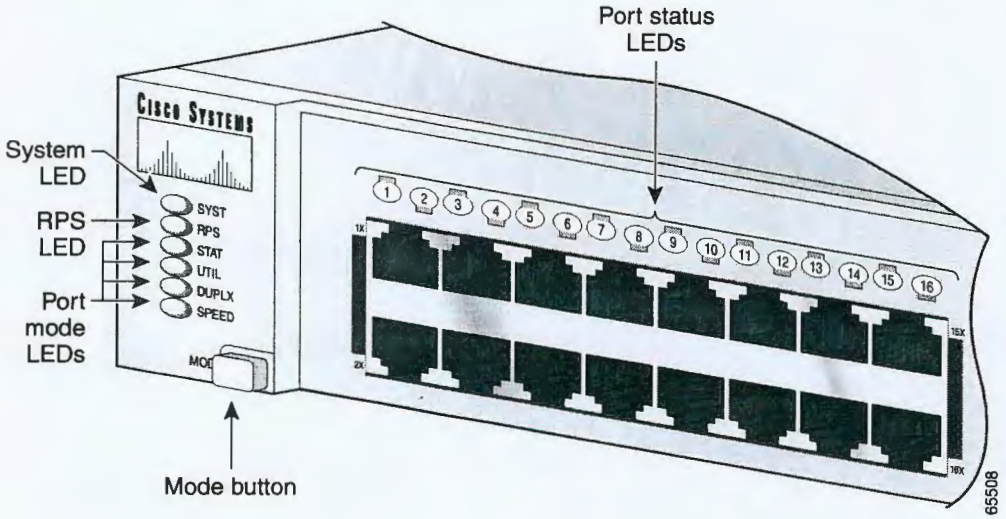
Figure 1-10 LEDs on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
0780
Fls. Nº
3690
Doc.

15.084
A-

Figure 1-11 LEDs on Catalyst 2950G-48-EI Switches



System LED

The system LED shows whether the system is receiving power and functioning properly. Table 1-3 lists the LED colors and meanings.

Table 1-3 System LED

Color	System Status
Off	System is not powered up.
Green	System is operating normally.
Amber	System is receiving power but is not functioning properly.

For information about the system LED colors during the power-on self-test (POST), see the "Running POST" section on page 2-29.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0781
Doc. 3690

15.033
A-

RPS LED

The RPS LED shows the RPS status. Table 1-4 lists the LED colors and meanings.

Table 1-4 RPS LED

Color	RPS Status
Off	RPS is off or is not installed.
Solid green	RPS is connected and ready to provide back-up power.
Flashing green	RPS is connected but is unavailable because it is providing power to another device (redundancy has been allocated to a neighboring device).
Solid amber	RPS is in standby mode or in a fault condition. Press the Standby/Active button on the RPS, and the LED should turn green. If it does not, the RPS fan could have failed. Contact Cisco Systems.
Flashing amber	The internal power supply in a switch has failed, and the RPS is providing power to the switch (redundancy has been allocated to this device).

For more information about the Cisco RPS 300, refer to the *Cisco RPS 300 Redundant Power System Hardware Installation Guide*.

Port Mode and Port Status LEDs

Each port has a port status LED, also called a port LED. These LEDs, as a group or individually, display information about the switch and the individual ports. The port modes (see Table 1-5) determine the type of information displayed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0782
Doc. 3690

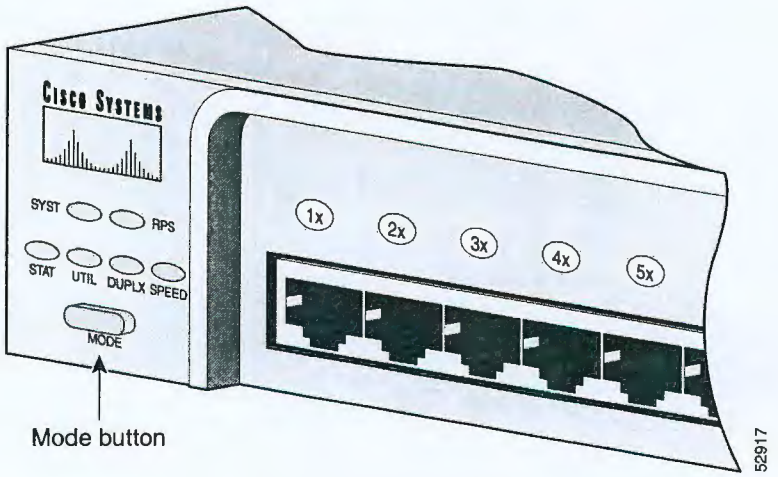
15.032
A.

Table 1-5 Port Mode LEDs

Mode LED	Port Mode	Description
STAT	Port status	The port status. This is the default mode.
UTIL	Switch utilization	The current bandwidth in use by the switch.
DUPLX	Port duplex mode	The port duplex mode: half duplex or full duplex.
SPEED	Port speed	The port operating speed: 10 or 100 Mbps for 10/100 ports and 10, 100, or 1000 Mbps for 10/100/1000 ports.

To select or change the port mode, press the Mode button (see Figure 1-12, Figure 1-13, and Figure 1-14) to highlight the mode that you want. Release the button to enable the highlighted mode.

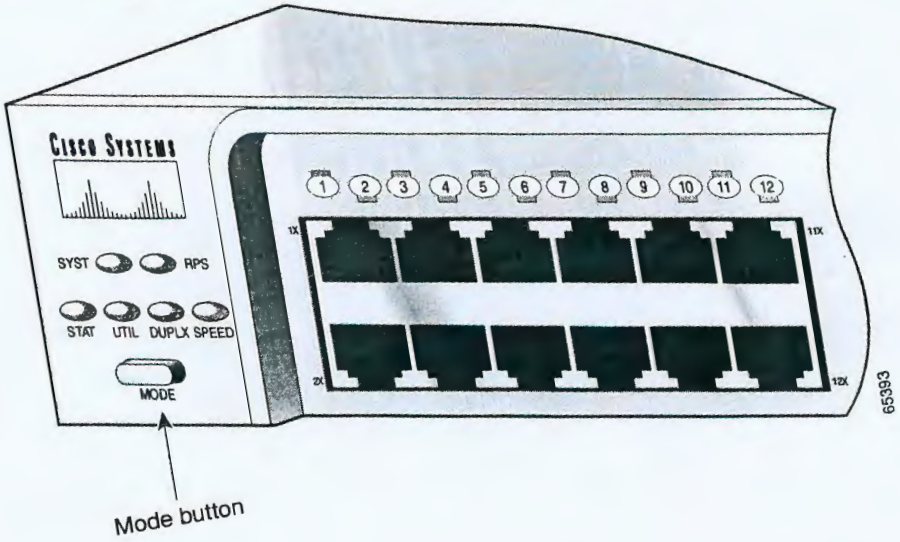
Figure 1-12 Changing the Port Mode on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0783
Doc. 3690

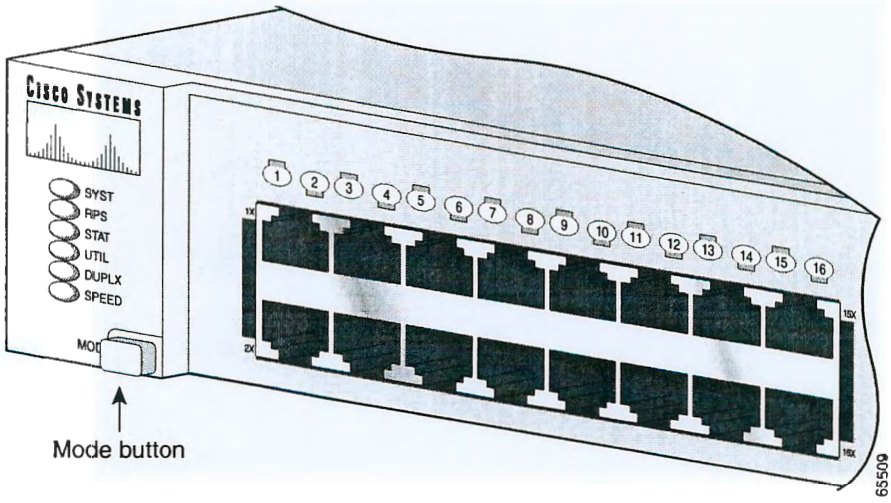
15.083
A-

Figure 1-13 Changing the Port Mode on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN
CPMI---CORREIOS
Fls. Nº 0784
Doc. 3690

Figure 1-14 Changing the Port Mode on Catalyst 2950G-48-EI Switches



ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0785
3690

15.079
A-

When you change the port mode, the meanings of the port LED colors change. Table 1-6 explains how to interpret these colors.

Table 1-6 Meaning of Port LED Colors in Different Modes

Port Mode	Color	Meaning
STAT (port status)	Off	No link.
	Solid green	Link present.
	Flashing green	Activity. Port is transmitting or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Solid amber	Port is not forwarding. Port was disabled by management, an address violation, or Spanning Tree Protocol (STP). **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the switch for possible loops.
UTIL (utilization)	Green	The current backplane utilization that is displayed over the amber LED background on a logarithmic scale.
	Amber	The maximum backplane utilization since the switch was powered on.
	Green and amber	See Figure 1-15 to Figure 1-18 for details. **Note** If the current utilization exceeds the maximum utilization, the maximum utilization is automatically updated.
DUPLX (half or full duplex)	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0586
Doc. 3690

15.078
A.

Table 1-6 Meaning of Port LED Colors in Different Modes (continued)

Port Mode	Color	Meaning
SPEED (speed)	10/100 ports	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	10/100/1000 ports	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	Flashing green	Port is operating at 1000 Mbps.
	1000BASE-X GBIC module ports	
	Off	Port is not operating.
	Green	Port is operating at 1000 Mbps.

For more information about GBIC LEDs, refer to your GBIC documentation.

Figure 1-15 to Figure 1-18 show the bandwidth utilization percentages displayed by the right-most LEDs.

If all LEDs on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the far-right LED is off, the switch is using more than 25 but less than 50 percent of the total bandwidth, and so on. If only the far-left LED is green, the switch is using less than 0.0488 percent of the total bandwidth. (See Figure 1-15.)

If all LEDs on Catalyst 2950G-12-EI switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the LED for GBIC module slot 2 is off, the switch is using more than 25 but less than 50 percent of the total bandwidth. If LEDs for both GBIC module slots are off, the switch is using less than 25 percent of the total bandwidth, and so on. (See Figure 1-16.)

If all LEDs on Catalyst 2950G-24-EI and 2950G-24-EI-DC switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the LED for GBIC module slot 2 is off, the switch is using more than 25 but less than 50 percent of the total bandwidth. If LEDs for both GBIC module slots are off, the switch is using less than 25 percent of the total bandwidth, and so on. (See Figure 1-17.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0787
Doc: 3690

If all LEDs on Catalyst 2950G-48-EI switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the LED for the upper GBIC module slot is off, the switch is using more than 25 but less than 50 percent of the total bandwidth. If LEDs for both GBIC module slots are off, the switch is using less than 25 percent of the total bandwidth, and so on. (See Figure 1-18.)

Figure 1-15 Bandwidth Utilization on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches

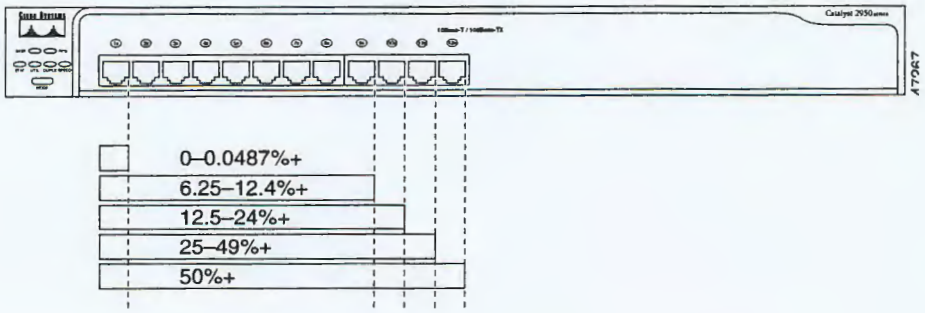


Figure 1-16 Bandwidth Utilization on Catalyst 2950G-12-EI Switches

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0788
Doc. 3690

15.016
A

Figure 1-17 Bandwidth Utilization on Catalyst 2950G-24-EI and 2950G-24-EI-DC Switches

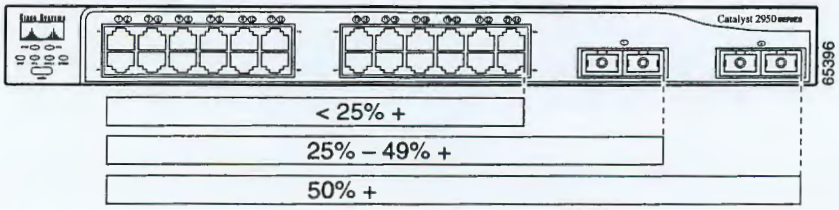
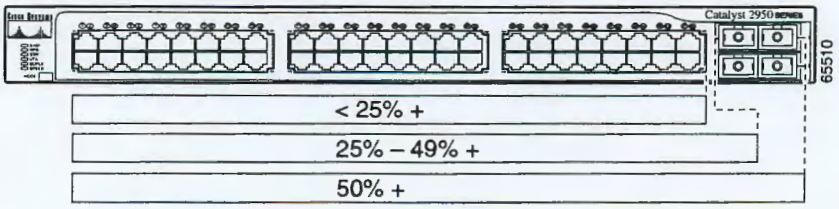


Figure 1-18 Bandwidth Utilization on Catalyst 2950G-48-EI Switches



Rear-Panel Description

Other than the Catalyst 2950G-24-EI-DC switch, the rear panel of a Catalyst 2950 switch has an AC power connector, an RPS connector, and an RJ-45 console port. (See Figure 1-19 and Figure 1-20.)

The rear panel of the Catalyst 2950G-24-EI-DC switch has a DC power connector (also referred to as the terminal block header), a DC ground lug, an RPS connector, and an RJ-45 console port. (See Figure 1-21.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0789
Doc. 3690

15.075
A:

Figure 1-19 Catalyst 2950 Switch Rear Panel

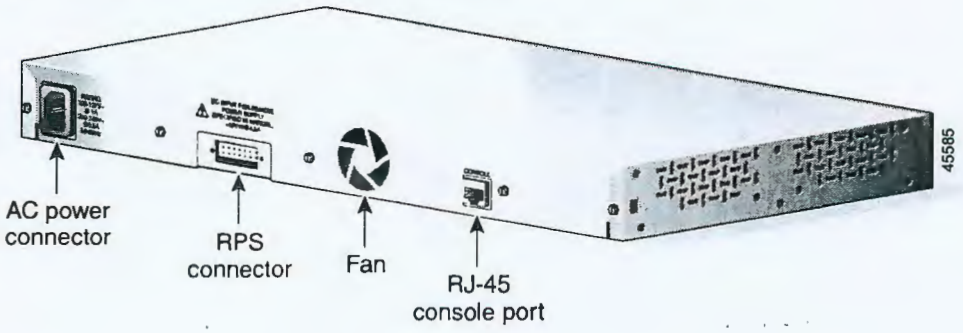
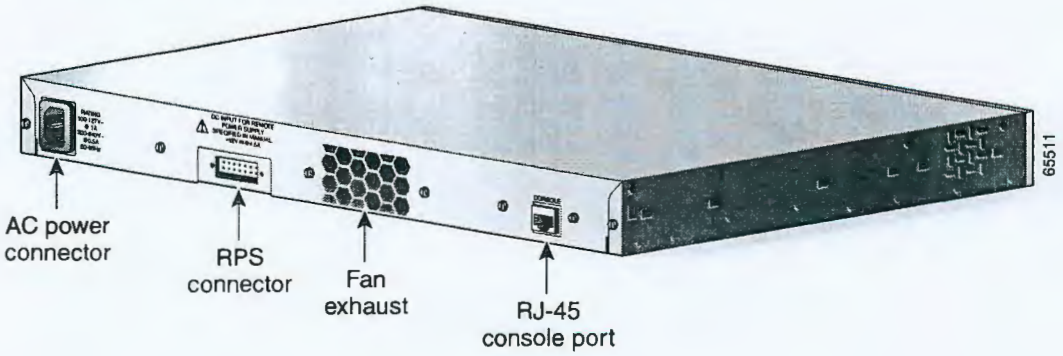


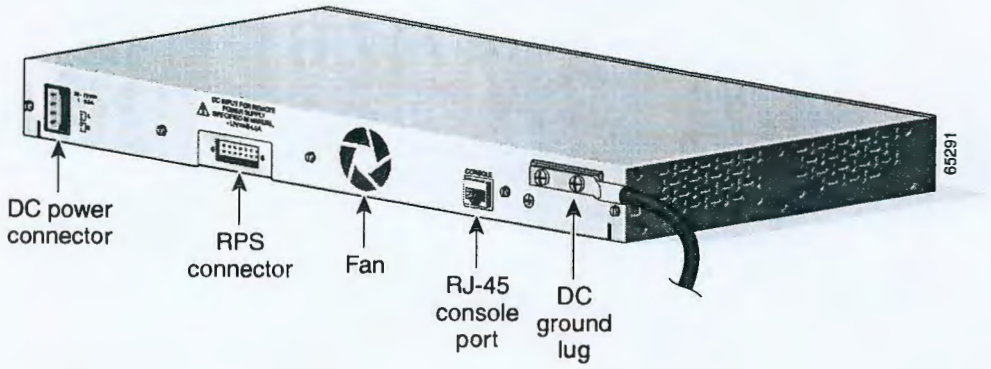
Figure 1-20 Catalyst 2950G-48-EI Switch Rear Panel



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 0790
Doc. 3690

15.074
A

Figure 1-21 Catalyst 2950G-24-EI-DC Switch Rear Panel



Power Connectors

You can provide power to a switch by using the AC internal power supply, the DC-input power source, or the Cisco RPS.

Internal Power Supply Connector

The internal AC power supply is an autoranging unit that supports input voltages between 100 and 240 VAC. Other than for the Catalyst 2950G-24-EI-DC switch, use the supplied AC power cord to connect the AC power connector to an AC power outlet.

DC Power Connector

The Catalyst 2950G-24-EI-DC switch has an internal DC-power converter. It has dual feeds (A and B) that are diode-OR-ed into a single power block. For installation instructions, see the "Connecting to DC Power" section on page 2-20.

Caution You must connect the Catalyst 2950G-24-EI-DC switch only to a DC-input power source that has an input supply voltage from –36 to –72 VDC. If the supply voltage is not in this range, the switch might not operate properly or might be damaged.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0791
Doc. 3690

Cisco RPS Connector

The RPS is a 300W redundant power system that can support six external network devices and provides DC power to one failed device at a time. It automatically senses when the internal power supply of a connected device fails and provides power to that device, preventing loss of network traffic.

Warning **Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle.**

For more information about the Cisco RPS 300, refer to the *Cisco RPS 300 Redundant Power System Hardware Installation Guide.*

Console Port

You can connect a switch to a PC through the console port and the supplied rollover cable and DB-9 adapter. If you want to connect a switch to a terminal, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco. For console-port and adapter-pinout information, see the "Cable and Adapter Specifications" section on page B-6.

Management Options

Catalyst 2950 switches offer these management options:

- Cluster Management Suite (CMS)

  CMS is made up of three web-based applications that you use to manage switches. You can use Cluster Builder, which includes Cluster View, and Cluster Manager to create, configure, and monitor switch clusters. You can also use Device Manager to manage individual and standalone switches. For more information, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* and the CMS online help.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0792
Doc 3690

15.072
A.

- IOS command-line interface (CLI)

  You can manage switches by using command-line entries. To access the CLI, connect a PC or terminal directly to the console port on the switch rear panel. If the switch is attached to your network, you can use a Telnet connection to manage the switch from a remote location. For more information, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

- CiscoView application

  You can use the CiscoView device-management application to set configuration parameters and to view switch status and performance information. This application, which you purchase separately, can be a standalone application or part of an Simple Network Management Protocol (SNMP) network-management platform. For more information, refer to the documentation that came with your CiscoView application.

- SNMP network management

  You can manage switches by using an SNMP-compatible management station running platforms such as HP OpenView and SunNet Manager. The switch supports a comprehensive set of MIB extensions and MIB II, the IEEE 802.1D bridge MIB, and four RMON groups. For more information, refer to the documentation that came with your SNMP application.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0793
Doc. 3690

Switch Tipo 2 doc 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
0794
Fls. Nº
3690
Doc.

15.070
CA.

Overview

This chapter provides information about these topics:

- Switch features
- Front- and rear-panel descriptions
- Management options

Features

The Catalyst 2950 switches are stackable Ethernet switches to which you can connect workstations and other network devices, such as servers, routers, and other switches. The switches can be deployed as backbone switches, aggregating 10BASE-T, 100BASE-TX, and Gigabit Ethernet traffic from other network devices. Refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* for examples showing how you might deploy the switches in your network.

Table 1-1 lists the switch features, and Figure 1-1 through Figure 1-8 show the Catalyst 2950 switches.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0795
Doc 3690

15.069

Table 1-1 Catalyst 2950 Switch Features

Feature	Description
Hardware	• Catalyst 2950-12 switch—12 10/100 Ethernet ports • Catalyst 2950-24 switch—24 10/100 Ethernet ports • Catalyst 2950C-24 switch—24 10/100 Ethernet ports and 2 100BASE-FX ports • Catalyst 2950G-12-EI—12 10/100 Ethernet ports and 2 GBIC[1]-based Gigabit Ethernet module slots • Catalyst 2950G-24-EI—24 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet module slots • Catalyst 2950G-24-EI-DC[2]—24 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet module slots with DC-input power • Catalyst 2950G-48-EI—48 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet module slots • Catalyst 2950T-24 switch—24 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports • On Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, and 2950G-48-EI switches, support for these GBIC modules: – 1000BASE-SX GBIC – 1000BASE-LX/LH GBIC – 1000BASE-ZX GBIC – GigaStack GBIC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 4796
3690
Doc.

Table 1-1 Catalyst 2950 Switch Features (continued)

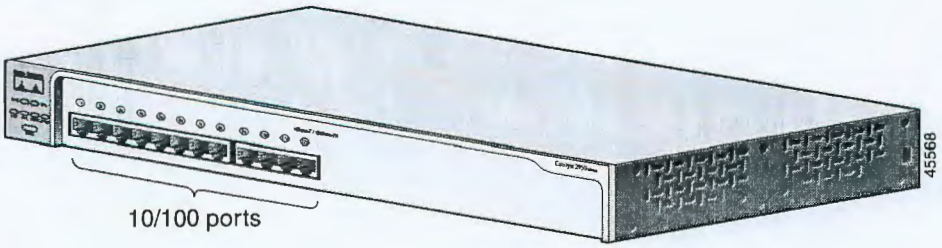
Feature	Description
Configuration	• Autonegotiates the speed and duplex settings on 10/100 ports and on 10/100/1000 ports • Supports only 100-Mbps and full-duplex settings on 100BASE-FX ports • Supports 8192 MAC addresses • Checks for errors on a received packet, determines the destination port, stores the packet in shared memory, and then forwards the packet to the destination port
Power redundancy	• Connection for an optional Cisco RPS 300 Redundant Power System (RPS) that uses AC[3] input and supplies DC output to the switch

1. GBIC = Gigabit Interface Converter
2. DC = direct current
3. AC = alternating current

Front-Panel Description

The switch front panel contains the ports, the LEDs, and the Mode button. Figure 1-1 to Figure 1-8 show the switches.

Figure 1-1 Catalyst 2950-12 Switch



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0797
Doc: 3690

Figure 1-2 Catalyst 2950-24 Switch

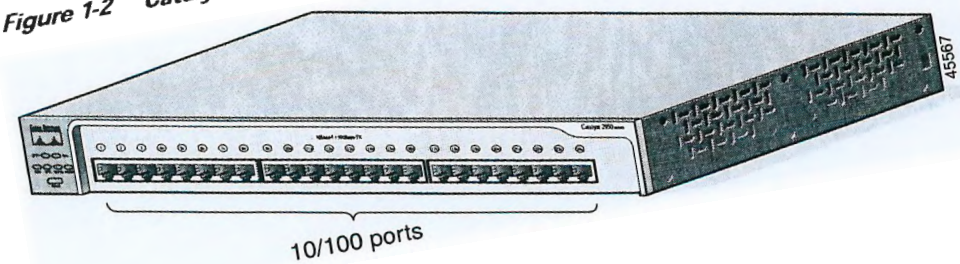


Figure 1-3 Catalyst 2950C-24 Switch

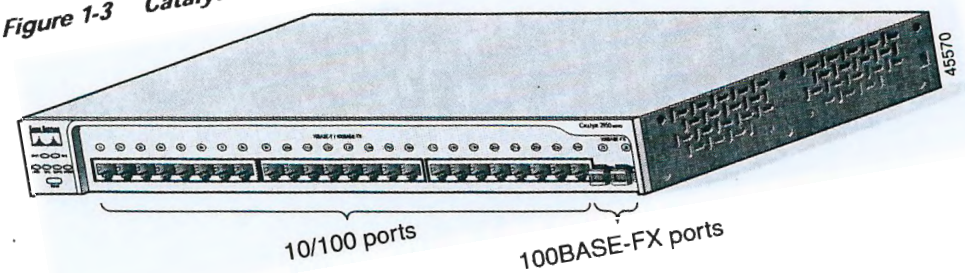
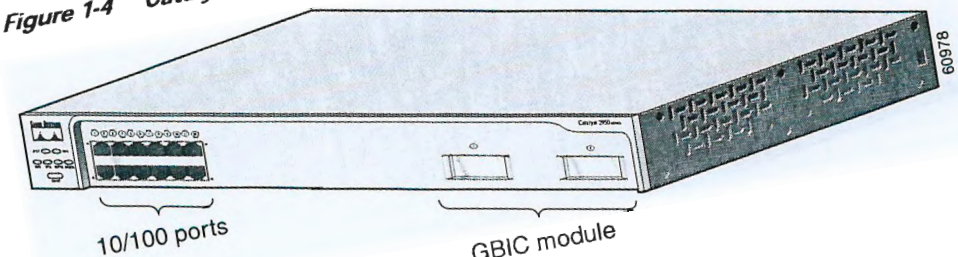


Figure 1-4 Catalyst 2950G-12-EI Switch



RQS nº 03/2005 - CN
CPMI - - CORREIOS
Fls. Nº 0798
3690
Doc.

15.066
LA.

Figure 1-5 Catalyst 2950G-24-EI Switch

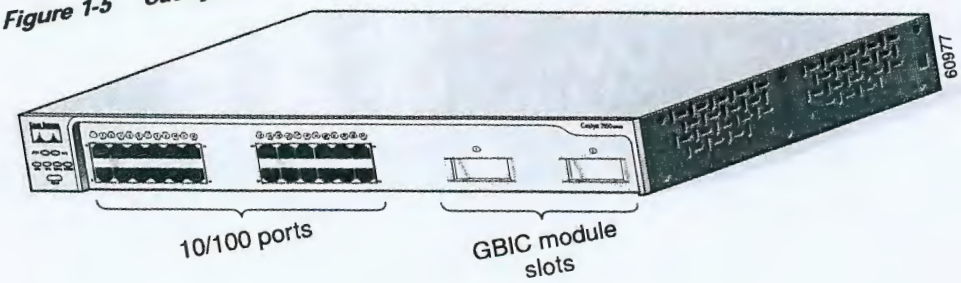


Figure 1-6 Catalyst 2950G-24-EI-DC Switch

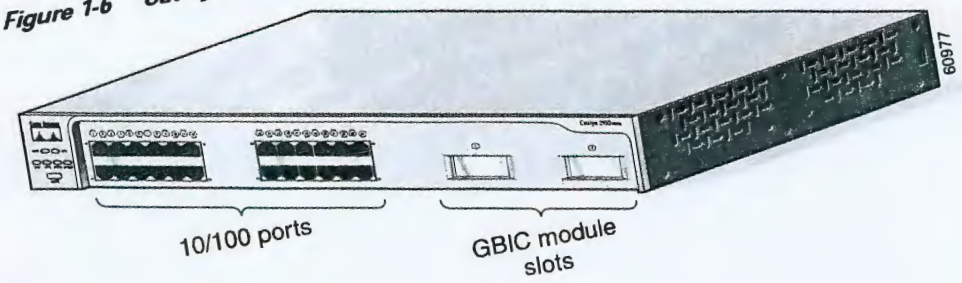
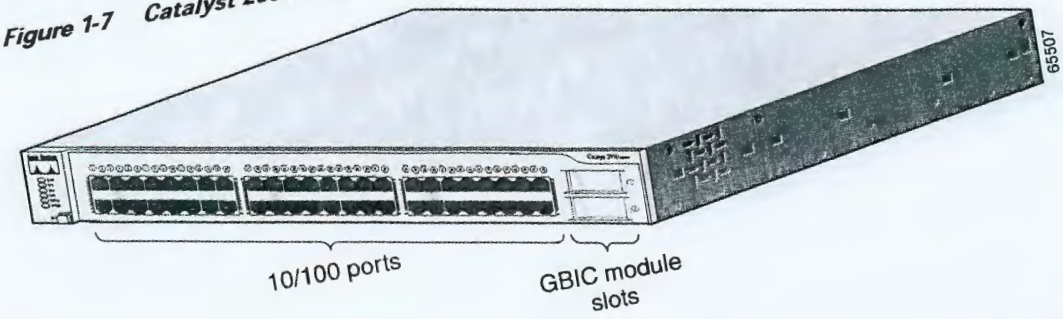


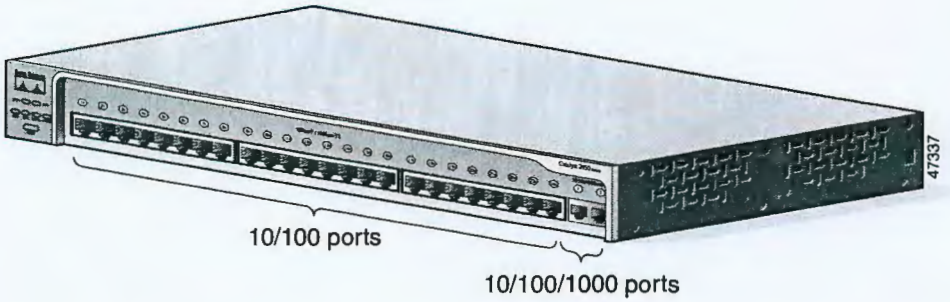
Figure 1-7 Catalyst 2950G-48-EI Switch



ECT II 0572001 - CN
CPMI - CORR
Fls. Nº 0799
Doc. 3690

15.065
JA

Figure 1-8 Catalyst 2950T-24 Switch



10/100 Ports

The 10/100 ports use RJ-45 connectors and twisted-pair cabling. The ports can connect to these devices:

- 10BASE-T-compatible devices, such as workstations and hubs, through standard RJ-45 connectors and two twisted-pair cabling. You can use Category 3, 4, or 5 cabling.
- 100BASE-TX-compatible devices, such as high-speed workstations, servers, hubs, routers, and other switches, through standard RJ-45 connectors and two or four twisted-pair, Category 5 cabling.

Note When connecting the switch to workstations, servers, and routers, be sure that the cable is a twisted-pair straight-through cable. When connecting the switch to hubs or other switches, use a twisted-pair crossover cable. Pinouts for the cables are described in Appendix B, "Connectors and Cables."

The 10/100 ports can be explicitly set to operate in any combination of half duplex, full duplex, 10 Mbps, or 100 Mbps. They can also be set for speed and duplex autonegotiation, compliant with IEEE 802.3U. In all cases, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-11157-02
Fls. Nº 0800
Doc. 3690

15.064
CA.

When set for autonegotiation, a port senses the speed and duplex settings of the attached device and advertises its own capabilities. If the attached device supports autonegotiation, the port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission, if the attached device supports it) and configures itself accordingly.

100BASE-FX Ports

The 100BASE-FX ports use 50/125- or 62.5/125-micron multimode fiber-optic cabling. These ports only operate at 100 Mbps in full-duplex mode.

In full-duplex mode (the default), the cable length from a switch to an attached device cannot exceed 6562 feet (2 kilometers).

You can connect a 100BASE-FX port to an SC or ST port on a target device by using one of the MT-RJ fiber-optic patch cables listed in Table 1-2. Use the Cisco part numbers in Table 1-2 to order the patch cables that you need.

Table 1-2 MT-RJ Patch Cables for 100BASE-FX Connections

Type	Cisco Part Number
1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

RQS nº 03/20
CPMI - CORREIOS
Fls. Nº 0801
Doc. 3690

10/100/1000 Ports

The 10/100/1000 ports on Catalyst 2950T-24 switches use RJ-45 connectors and twisted-pair cabling. The ports can connect to these devices:

- 10BASE-T-compatible devices, such as workstations and hubs, through standard RJ-45 connectors and two or four twisted-pair, Category 5 cabling.
- 100BASE-TX-compatible devices, such as high-speed workstations, servers, hubs, routers, and other switches, through standard RJ-45 connectors and two or four twisted-pair, Category 5 cabling.
- 1000BASE-T-compatible devices, such as high-speed workstations, servers, hubs, routers, and other switches, through standard RJ-45 connectors and four twisted-pair, Category 5 cabling.

Note When connecting to a 1000BASE-T-compatible device, be sure to use a four twisted-pair, Category 5 cable.

Note When connecting the switch to workstations, servers, and routers, be sure that the cable is a twisted-pair straight-through cable. When connecting the switch to hubs or other switches, use a twisted-pair crossover cable. Pinouts for the cables are described in Appendix B, "Connectors and Cables."

The 10/100/1000 ports on Catalyst 2950T-24 switches can be explicitly set to operate at 10 or 100 Mbps in half- or full-duplex mode or at 1000 Mbps in full-duplex mode. The default duplex setting is full duplex. They can also be set for speed and duplex autonegotiation, compliant with IEEE 802.3AB. In all cases, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0802
Doc. 3690

GBIC Module Ports

The GBIC module slots support these modules:

- 1000BASE-SX GBIC module for fiber-optic connections that cannot exceed 1804 feet (550 meters).
- 1000BASE-LX/LH GBIC module for fiber-optic connections that cannot exceed 32,810 feet (10 kilometers).
- 1000BASE-ZX GBIC module for fiber-optic connections that cannot exceed 328,100 feet (100 kilometers).
- GigaStack GBIC module for creating a 1-Gbps stack configuration of up to nine supported switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to nine half-duplex links (in a stack configuration) to other Gigabit Ethernet devices. Using the required Cisco proprietary signaling and cabling, the GigaStack GBIC-to-GigaStack GBIC connection cannot exceed 3 feet (1 meter).

For more information about these GBICs, refer to your GBIC documentation.

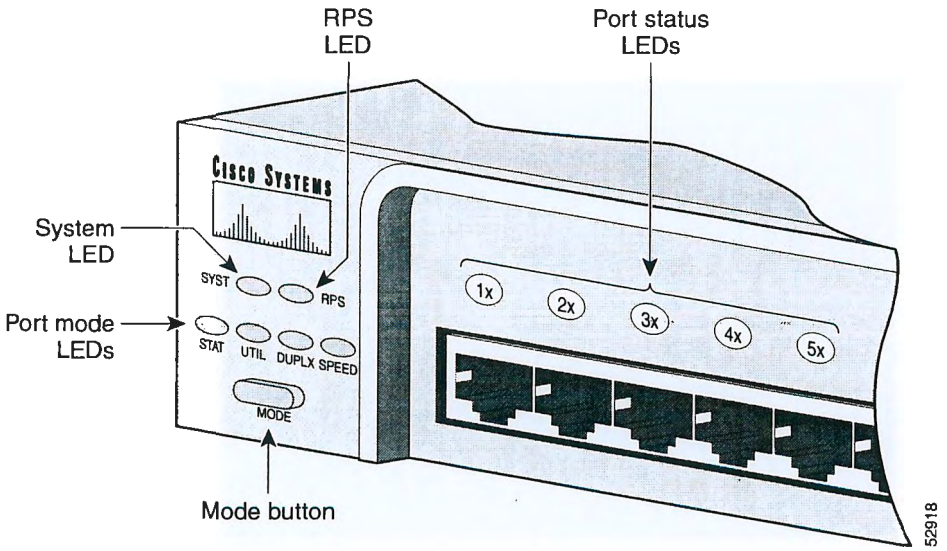
LEDs

You can use the LEDs to monitor switch activity and performance. Figure 1-9, Figure 1-10, and Figure 1-11 show the location of the LEDs and the Mode button that you use to select the port mode. Changing the port mode changes the information provided by each port status LED.

All of the LEDs described in this section except the utilization meter (UTIL) are visible in the Cluster Management Suite (CMS). The *Catalyst 2950 Desktop Switch Software Configuration Guide* describes how to use CMS to manage individual switches and switch clusters.

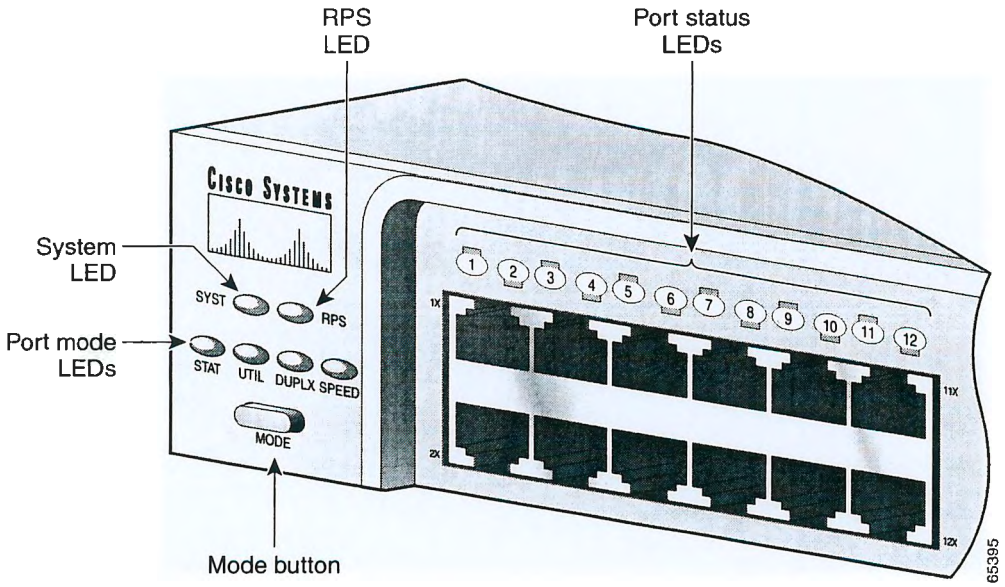
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0803
Doc 3690

Figure 1-9 LEDs on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches



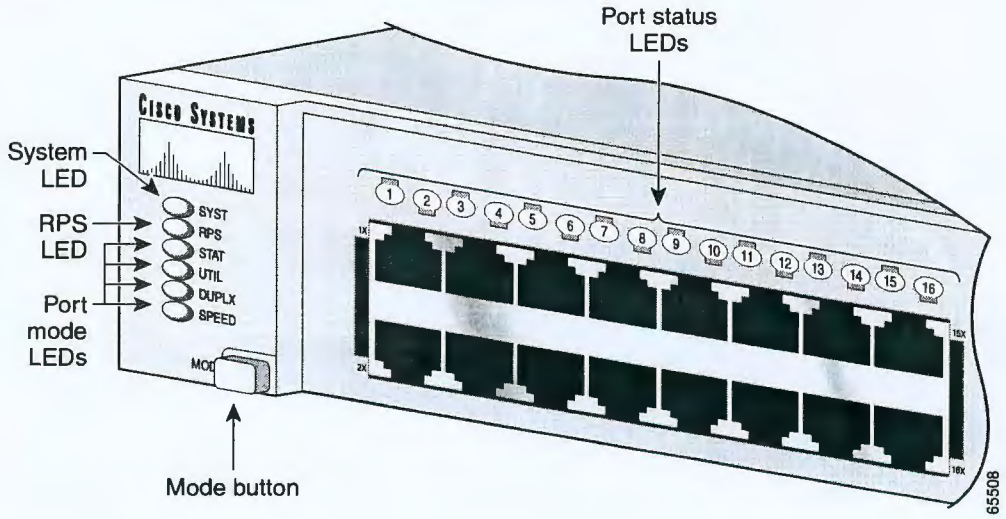
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0804
Doc. 3690

Figure 1-10 LEDs on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
0805
Fls. Nº
Doc. 3690

Figure 1-11 LEDs on Catalyst 2950G-48-EI Switches



System LED

The system LED shows whether the system is receiving power and functioning properly. Table 1-3 lists the LED colors and meanings.

Table 1-3 System LED

Color	System Status
Off	System is not powered up.
Green	System is operating normally.
Amber	System is receiving power but is not functioning properly.

For information about the system LED colors during the power-on self-test (POST), see the "Running POST" section on page 2-29.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0806
Doc. 3690

15.053
A.

RPS LED

The RPS LED shows the RPS status. Table 1-4 lists the LED colors and meanings.

Table 1-4 RPS LED

Color	RPS Status
Off	RPS is off or is not installed.
Solid green	RPS is connected and ready to provide back-up power.
Flashing green	RPS is connected but is unavailable because it is providing power to another device (redundancy has been allocated to a neighboring device).
Solid amber	RPS is in standby mode or in a fault condition. Press the Standby/Active button on the RPS, and the LED should turn green. If it does not, the RPS fan could have failed. Contact Cisco Systems.
Flashing amber	The internal power supply in a switch has failed, and the RPS is providing power to the switch (redundancy has been allocated to this device).

For more information about the Cisco RPS 300, refer to the *Cisco RPS 300 Redundant Power System Hardware Installation Guide*.

Port Mode and Port Status LEDs

Each port has a port status LED, also called a port LED. These LEDs, as a group or individually, display information about the switch and the individual ports. The port modes (see Table 1-5) determine the type of information displayed.

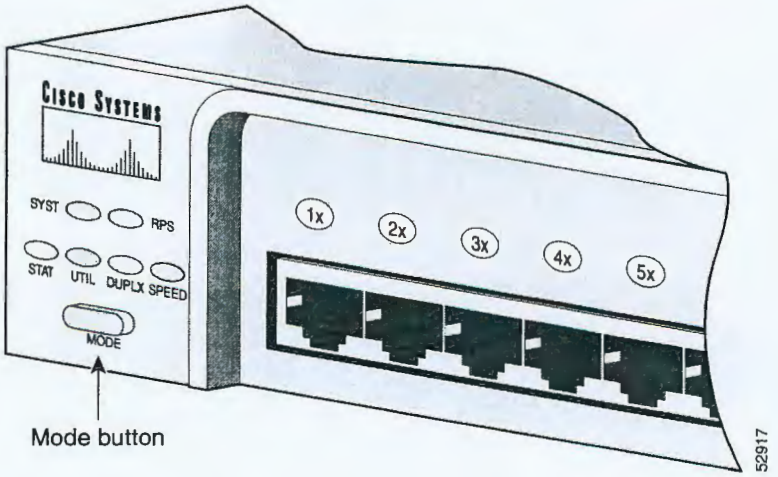
RQS nº 03/2005 - CN
CPMI - CORREIOS
0807
Fls. Nº
Doc. 3690

Table 1-5 Port Mode LEDs

Mode LED	Port Mode	Description
STAT	Port status	The port status. This is the default mode.
UTIL	Switch utilization	The current bandwidth in use by the switch.
DUPLX	Port duplex mode	The port duplex mode: half duplex or full duplex.
SPEED	Port speed	The port operating speed: 10 or 100 Mbps for 10/100 ports and 10, 100, or 1000 Mbps for 10/100/1000 ports.

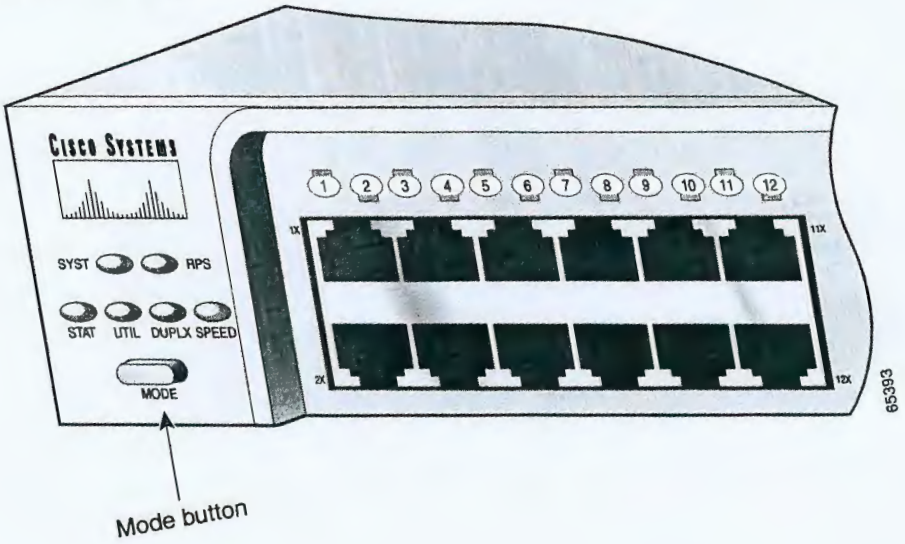
To select or change the port mode, press the Mode button (see Figure 1-12, Figure 1-13, and Figure 1-14) to highlight the mode that you want. Release the button to enable the highlighted mode.

Figure 1-12 Changing the Port Mode on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0808
Doc 3690

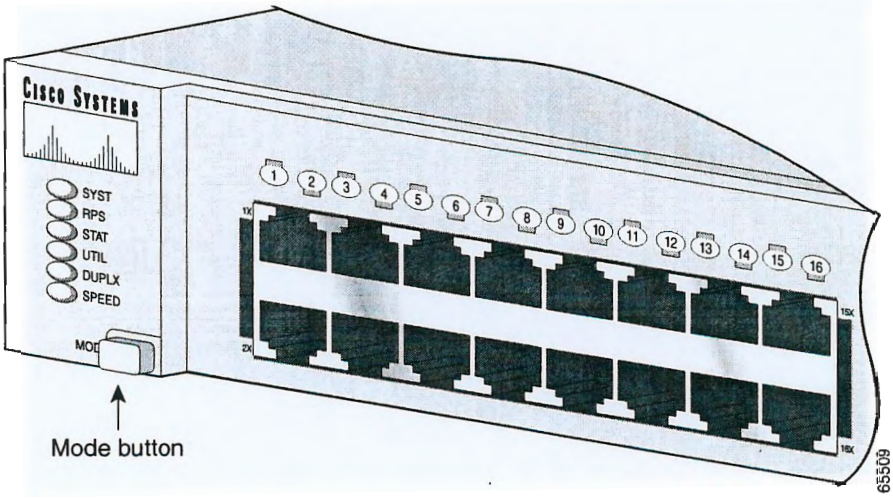
Figure 1-13 Changing the Port Mode on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0809
Doc. 3690

15.055
4

Figure 1-14 Changing the Port Mode on Catalyst 2950G-48-EI Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0810
Doc. 3690

When you change the port mode, the meanings of the port LED colors change. Table 1-6 explains how to interpret these colors.

Table 1-6 Meaning of Port LED Colors in Different Modes

Port Mode	Color	Meaning
STAT (port status)	Off	No link.
	Solid green	Link present.
	Flashing green	Activity. Port is transmitting or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Solid amber	Port is not forwarding. Port was disabled by management, an address violation, or Spanning Tree Protocol (STP). **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the switch for possible loops.
UTIL (utilization)	Green	The current backplane utilization that is displayed over the amber LED background on a logarithmic scale.
	Amber	The maximum backplane utilization since the switch was powered on.
	Green and amber	See Figure 1-15 to Figure 1-18 for details. **Note** If the current utilization exceeds the maximum utilization, the maximum utilization is automatically updated.
DUPLX (half or full duplex)	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0811
Doc. 3690

Table 1-6 Meaning of Port LED Colors in Different Modes (continued)

Port Mode	Color	Meaning
SPEED (speed)	10/100 ports	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	10/100/1000 ports	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	Flashing green	Port is operating at 1000 Mbps.
	1000BASE-X GBIC module ports	
	Off	Port is not operating.
	Green	Port is operating at 1000 Mbps.

For more information about GBIC LEDs, refer to your GBIC documentation.

Figure 1-15 to Figure 1-18 show the bandwidth utilization percentages displayed by the right-most LEDs.

If all LEDs on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the far-right LED is off, the switch is using more than 25 but less than 50 percent of the total bandwidth, and so on. If only the far-left LED is green, the switch is using less than 0.0488 percent of the total bandwidth. (See Figure 1-15.)

If all LEDs on Catalyst 2950G-12-EI switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the LED for GBIC module slot 2 is off, the switch is using more than 25 but less than 50 percent of the total bandwidth. If LEDs for both GBIC module slots are off, the switch is using less than 25 percent of the total bandwidth, and so on. (See Figure 1-16.)

If all LEDs on Catalyst 2950G-24-EI and 2950G-24-EI-DC switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the LED for GBIC module slot 2 is off, the switch is using more than 25 but less than 50 percent of the total bandwidth. If LEDs for both GBIC module slots are off, the switch is using less than 25 percent of the total bandwidth, and so on. (See Figure 1-17.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0812
Doc. 3690

15.052
A.

If all LEDs on Catalyst 2950G-48-EI switches are green (no amber showing), the switch is using 50 percent or more of the total bandwidth. If the LED for the upper GBIC module slot is off, the switch is using more than 25 but less than 50 percent of the total bandwidth. If LEDs for both GBIC module slots are off, the switch is using less than 25 percent of the total bandwidth, and so on. (See Figure 1-18.)

Figure 1-15 Bandwidth Utilization on Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches

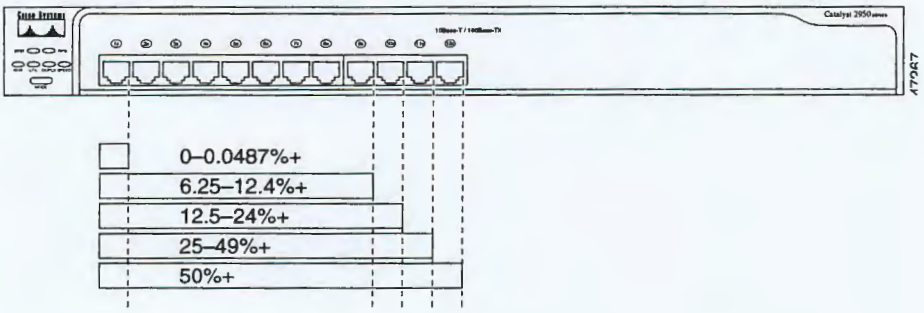


Figure 1-16 Bandwidth Utilization on Catalyst 2950G-12-EI Switches

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0813
Doc. 3690

15.051
4

Figure 1-17 Bandwidth Utilization on Catalyst 2950G-24-EI and 2950G-24-EI-DC Switches

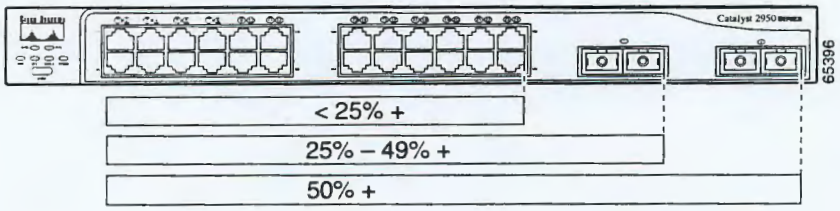
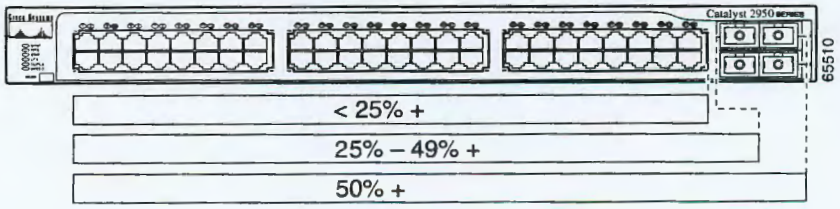


Figure 1-18 Bandwidth Utilization on Catalyst 2950G-48-EI Switches



Rear-Panel Description

Other than the Catalyst 2950G-24-EI-DC switch, the rear panel of a Catalyst 2950 switch has an AC power connector, an RPS connector, and an RJ-45 console port. (See Figure 1-19 and Figure 1-20.)

The rear panel of the Catalyst 2950G-24-EI-DC switch has a DC power connector (also referred to as the terminal block header), a DC ground lug, an RPS connector, and an RJ-45 console port. (See Figure 1-21.)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls 0814
Doc. 3690

Figure 1-19 Catalyst 2950 Switch Rear Panel

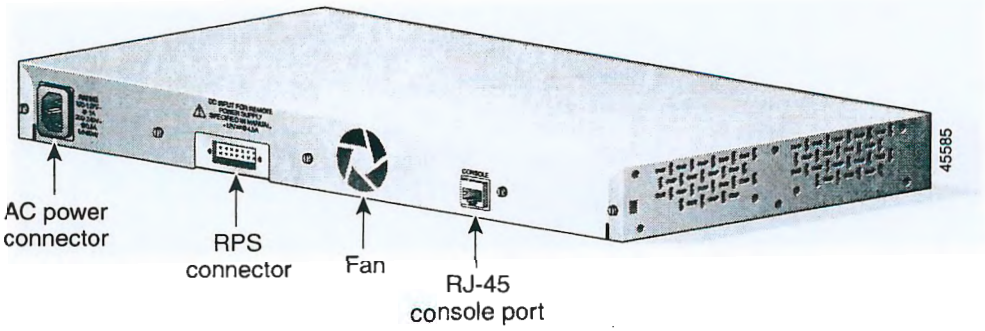
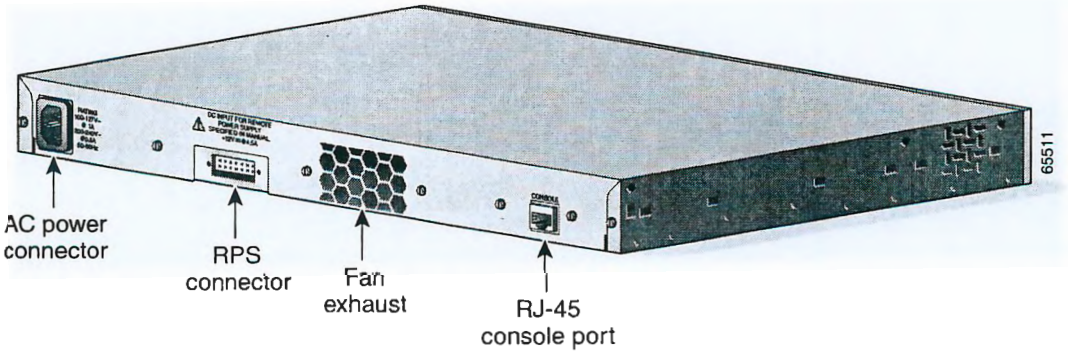


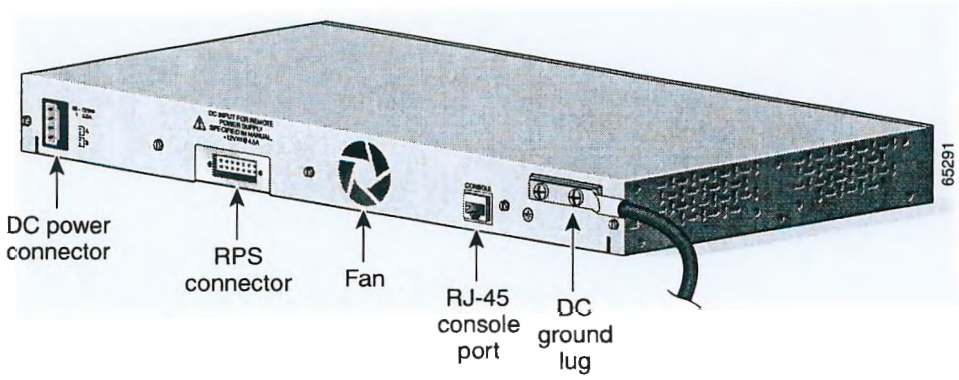
Figure 1-20 Catalyst 2950G-48-EI Switch Rear Panel



RQS nº 03/2005 - CN
CPMI - CORREIOS
0815
Fls. Nº
3690
Doc.

15.049
A.

Figure 1-21 Catalyst 2950G-24-EI-DC Switch Rear Panel



Power Connectors

You can provide power to a switch by using the AC internal power supply, the DC-input power source, or the Cisco RPS.

Internal Power Supply Connector

The internal AC power supply is an autoranging unit that supports input voltages between 100 and 240 VAC. Other than for the Catalyst 2950G-24-EI-DC switch, use the supplied AC power cord to connect the AC power connector to an AC power outlet.

DC Power Connector

The Catalyst 2950G-24-EI-DC switch has an internal DC-power converter. It has dual feeds (A and B) that are diode-OR-ed into a single power block. For installation instructions, see the "Connecting to DC Power" section on page 2-20.

Caution You must connect the Catalyst 2950G-24-EI-DC switch only to a DC-input power source that has an input supply voltage from –36 to –72 VDC. If the supply voltage is not in this range, the switch might not operate properly or might be damaged.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 0816
Doc. 3690

Cisco RPS Connector

The RPS is a 300W redundant power system that can support six external network devices and provides DC power to one failed device at a time. It automatically senses when the internal power supply of a connected device fails and provides power to that device, preventing loss of network traffic.

Warning **Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle.**

For more information about the Cisco RPS 300, refer to the *Cisco RPS 300 Redundant Power System Hardware Installation Guide.*

Console Port

You can connect a switch to a PC through the console port and the supplied rollover cable and DB-9 adapter. If you want to connect a switch to a terminal, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco. For console-port and adapter-pinout information, see the "Cable and Adapter Specifications" section on page B-6.

Management Options

Catalyst 2950 switches offer these management options:

- Cluster Management Suite (CMS)

  CMS is made up of three web-based applications that you use to manage switches. You can use Cluster Builder, which includes Cluster View, and Cluster Manager to create, configure, and monitor switch clusters. You can also use Device Manager to manage individual and standalone switches. For more information, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide* and the CMS online help.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0817
Doc. 3690

- IOS command-line interface (CLI)

  You can manage switches by using command-line entries. To access the CLI, connect a PC or terminal directly to the console port on the switch rear panel. If the switch is attached to your network, you can use a Telnet connection to manage the switch from a remote location. For more information, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

- CiscoView application

  You can use the CiscoView device-management application to set configuration parameters and to view switch status and performance information. This application, which you purchase separately, can be a standalone application or part of an Simple Network Management Protocol (SNMP) network-management platform. For more information, refer to the documentation that came with your CiscoView application.

- SNMP network management

  You can manage switches by using an SNMP-compatible management station running platforms such as HP OpenView and SunNet Manager. The switch supports a comprehensive set of MIB extensions and MIB II, the IEEE 802.1D bridge MIB, and four RMON groups. For more information, refer to the documentation that came with your SNMP application.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0818
Doc. 3690

roriz@IBM-297NYWD11S3

15.0

Job Title: SWITCH_TIPO2_doc3.pdf

Time Queued: Thu Jul 24 03:34:30 2003
Time Printed: Thu Jul 24 04:08:07 2003

Submitted By: roriz@IBM-297NYWD11S3

roriz@IBM-297NYWD11S3

Need help? Call your local NCO HelpDesk.

PIO_DEV: ibm@brbrap7a#ibmNetPrinter (ibm4320) @ brbraprt01

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0819
Doc. 3690

Installation

This chapter describes how to install your switch, interpret the power-on self-test (POST), and connect the switch to other devices. Read these topics and perform the procedures in this order:

- Preparing for Installation, page 2-2
- Installing the Switch in a Rack, page 2-9
- Installing the Switch on a Table, Shelf, or Desk, page 2-20
- Installing the GBIC Modules, page 2-20
- Powering On the Switch, page 2-22
- Connecting to DC Power, page 2-23
- Running POST, page 2-32
- Connecting to 10/100 and 10/100/1000 Ports, page 2-33
- Connecting to 100BASE-FX and 1000BASE-SX Ports, page 2-37
- Connecting to GBIC Module Ports, page 2-38
- Connecting a PC or a Terminal to the Console Port, page 2-43
- Where to Go Next, page 2-45

RQS n - CN
CPMI - CORREIOS
0820
Fls. Nº
3690
Doc.

15.044
A.

Preparing for Installation

This section provides information about these topics:

- Warnings, page 2-2
- EMC Regulatory Statements, page 2-4
- Installation Guidelines, page 2-6
- Verifying Package Contents, page 2-7

Warnings

These warnings are translated into several languages in Appendix C, "Translated Safety Warnings."

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.**

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Unplug the power cord before you work on a system that does not have an on/off switch.**

Warning **Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.**

ECT 78-1115/2005 - CN
CPMI - CORREIOS
Fls. 0821
Doc. 3690

15.043
A.

Warning The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

Warning To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Warning When installing the unit, always make the ground connection first and disconnect it last.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning Ultimate disposal of this product should be handled according to all national laws and regulations.

Warning Attach only the Cisco RPS (model PWR300-AC-RPS-N1) to the RPS receptacle.

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls 0822
3690
Doc.

15042
A-

Warning **Class 1 laser product**

Warning **Avoid exposure to the laser beam.**

EMC Regulatory Statements

This section includes specific regulatory statements about the Catalyst 2950 switches.

U.S.A.

U.S. regulatory information for this product is in the front matter of this manual.

Taiwan

This is a Class A Information product. When used in a residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

RQS nº 03/2005 - CN
CPMI - CORREIOS
0823
Fls. Nº
3690
Doc.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

46464

Korea

Warning **This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type.**

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

15.041 A.
ROS nº 03/2 2-5
CPMI - CORREIOS
Fls. Nº 0824
3690
Doc.

15.040

Hungary

This equipment is a Class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

Figyelmeztetés a felhasználói kézikönyv számára:
Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleloen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Installation Guidelines

When determining where to place the switch, observe these guidelines.

- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- For 100BASE-FX ports, the cable length from a switch to an attached device cannot exceed 6562 feet (2 kilometers).
- For 1000BASE-SX ports and 1000BASE-SX GBIC module ports, the cable length from a switch to an attached device cannot exceed 1804 feet (550 meters).
- For 1000BASE-LX/LH GBIC module ports, the cable length from a switch to an attached device cannot exceed 32,810 feet (10 kilometers).
- For 1000BASE-ZX GBIC module ports, the cable length from a switch to an attached device cannot exceed 328,100 feet (100 kilometers).
- For 1000BASE-T GBIC module ports, the cable length from switch to an attached device cannot exceed 328 feet (100 meters).
- For Coarse Wave Division Multiplexing (CWDM) GBIC module ports, the cable length from a switch to an attached device cannot exceed 393,719 feet (120 kilometers). For specific cable lengths, refer to the CWDM GBIC module documentation.
- For GigaStack GBIC module ports, the cable length from a switch to an attached device cannot exceed 3 feet (1 meter).

RQS nº 03/2005 - CN
CPMI - CORREIOS
0825
Fls. Nº
3690
Doc.

- Operating environment is within the ranges listed in Appendix A, "Technical Specifications."
- Clearance to front and rear panels meet these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Rear-panel AC power connector is within reach of an AC power outlet.
  - Rear-panel direct current (DC) power connector is within reach of a circuit breaker.
- Airflow around the switch and through the vents is unrestricted.
- Temperature around the unit does not exceed 113°F (45°C).

Note If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.

Verifying Package Contents

Note Carefully remove the contents from the shipping container, and check each item for damage. If any item is missing or damaged, contact your Cisco representative or reseller for support. Return all packing materials to the shipping container and save them.

The switch is shipped with these items:

- This *Catalyst 2950 Desktop Switch Hardware Installation Guide*
- *Where to Find the Catalyst 2950 Documentation* flyer
- Cisco Documentation CD-ROM
- AC power cord

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0826
3690
Doc.

15.038
A-

- Mounting kit containing these items:
  - Four rubber feet for mounting the switch on a table, shelf, or desk
  - Two 19-inch or 24-inch rack-mounting brackets
  - Six number-8 Phillips flat-head screws for attaching the brackets to the switch
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Four number-12 Phillips machine screws for attaching the brackets to a rack
  - One cable guide and one black Phillips machine screw for attaching the cable guide to one of the mounting brackets
- DC-switch kit containing these items:
  - One DC terminal block plug (also called a terminal block header)
  - One ground lug
  - Two number-10-32 screws for attaching the ground lug to the switch
  - Two 23-inch rack-mounting brackets (with 1-inch spacing for telco racks)
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Two number-12 Phillips machine screws for attaching the brackets to a rack

Note The DC-switch kit ships only with the Catalyst 2950G-24-EI-DC switch.

- One RJ-45-to-DB-9 adapter cable
- Cisco Information Packet, containing safety and support information

If you want to connect a terminal to the switch console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0827
Fls. Nº
3690
Doc.

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on a target device by using one of the MT-RJ fiber-optic patch cables listed in Table 2-1. Use the Cisco part numbers in Table 2-1 to order the patch cables that you need.

Table 2-1 MT-RJ Patch Cables for 100BASE-FX and 1000BASE-SX Connections

Type	Cisco Part Number
1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

Installing the Switch in a Rack

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Note Figure 2-1 to Figure 2-17 show the Catalyst 2950-24, 2950G-24-EI-DC, and 2950G-48-EI switches as examples. You can install other Catalyst 2950 switches in a rack as shown in these illustrations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0828
Doc. 3690

To install the switch in a 19-, 23-, or 24-inch rack, follow these steps:

- Attaching the Brackets to the Switch, page 2-10
- Mounting the Switch in a Rack, page 2-19
- Attaching the Optional Cable Guide, page 2-19

Note Installing the Catalyst 2950G-48-EI switch in a 23-inch or 24-inch rack requires an optional bracket kit not included with the switch. You can order a kit containing the 23-inch or 24-inch rack-mounting brackets and hardware from Cisco (part number RCKMNT-1RU=).

Attaching the Brackets to the Switch

The bracket orientation and the screws that you use depend on whether you are attaching the brackets to a 19-, 23-, or 24-inch rack. Follow these guidelines:

- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 19-inch rack, use two Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 2-1, Figure 2-2, and Figure 2-3.
- When mounting a Catalyst 2950G-48-EI switch in a 19-inch rack, use three Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 2-4, Figure 2-5, and Figure 2-6.
- When mounting a Catalyst 2950G-24-EI-DC switch in a 23-inch rack, use two Phillips truss-head screws to attach the 23-inch bracket to the switch. See Figure 2-7, Figure 2-8, and Figure 2-9.
- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 24-inch rack, use two Phillips truss-head screws to attach the 19- or 24-inch bracket to the switch. See Figure 2-10, Figure 2-11, and Figure 2-12.
- When mounting a Catalyst 2950G-48-EI switch in a 24-inch rack, use three Phillips flat-head screws to attach the 24-inch bracket (part number RCKMNT-1RU=) to the switch. See Figure 2-13, Figure 2-14, and Figure 2-15.

Figure 2-1 to Figure 2-15 show how to attach a bracket to one side of the switch. Follow the same steps to attach the second bracket to the opposite side of the switch.

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-14157-03
Fls. Nº 0829
Doc. 3690

15.035
J.

Figure 2-1 Attaching Brackets on the Switch in a 19-Inch Rack (Front Panel Forward)

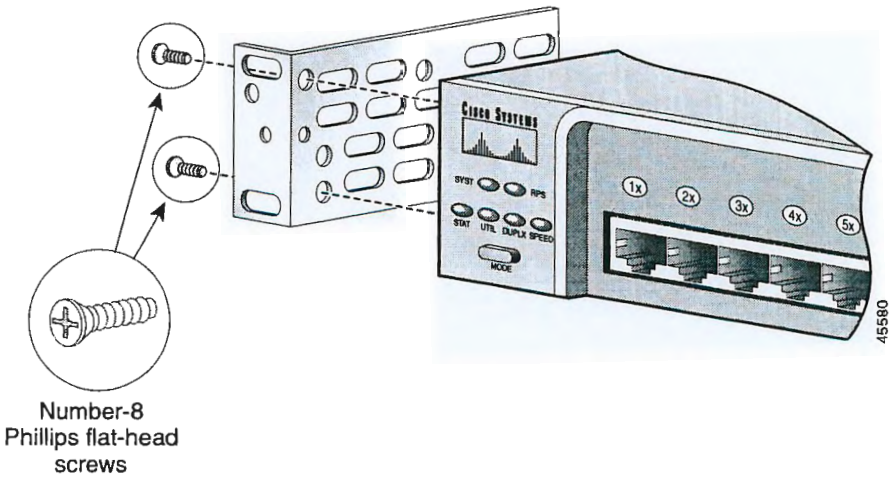
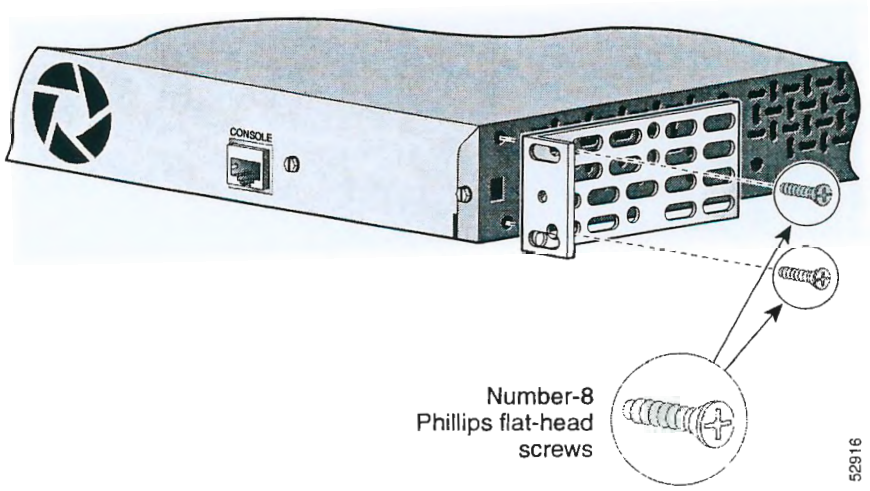


Figure 2-2 Attaching Brackets on the Switch in a 19-Inch Rack (Rear Panel Forward)



RQS nº 03/2005 - CN
CPMI - CORREIOS
0230
Fls. Nº
3690
Doc.

15.034
4.

Figure 2-3 Attaching Brackets on the Switch in a 19-Inch Telco Rack

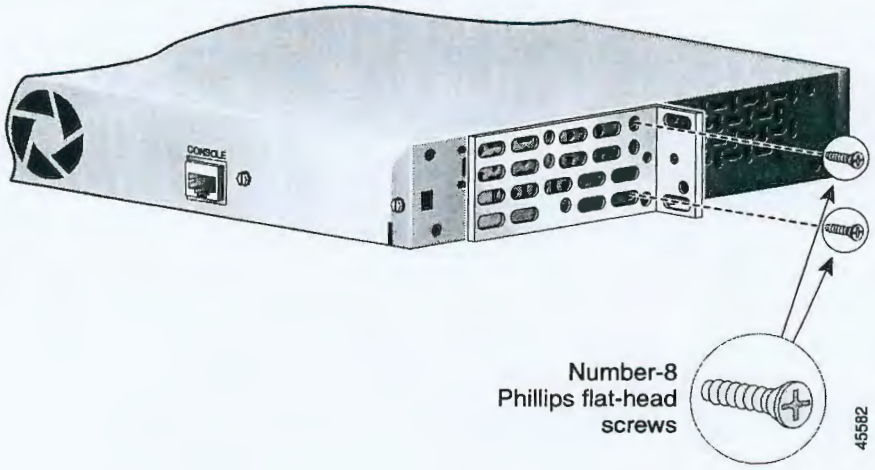
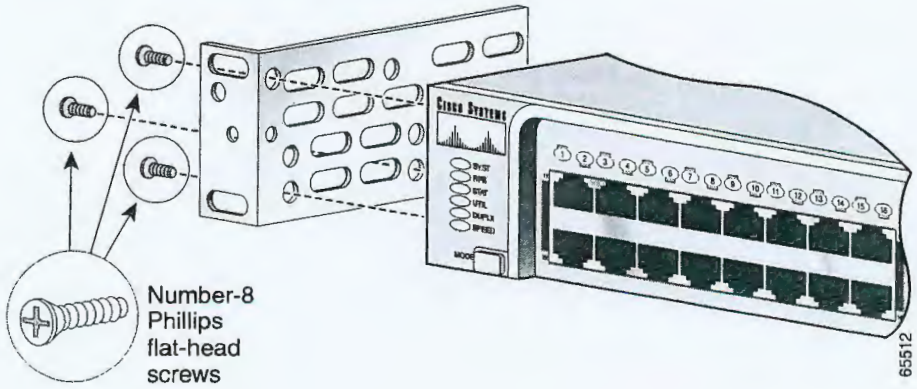


Figure 2-4 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Front Panel Forward)



78-11157-03
RQS nº 03/2005 - CN
CPMI - CORREIOS
0831
Fls. Nº
Doc. 3690

15.033
A.

Figure 2-5 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Rear Panel Forward)

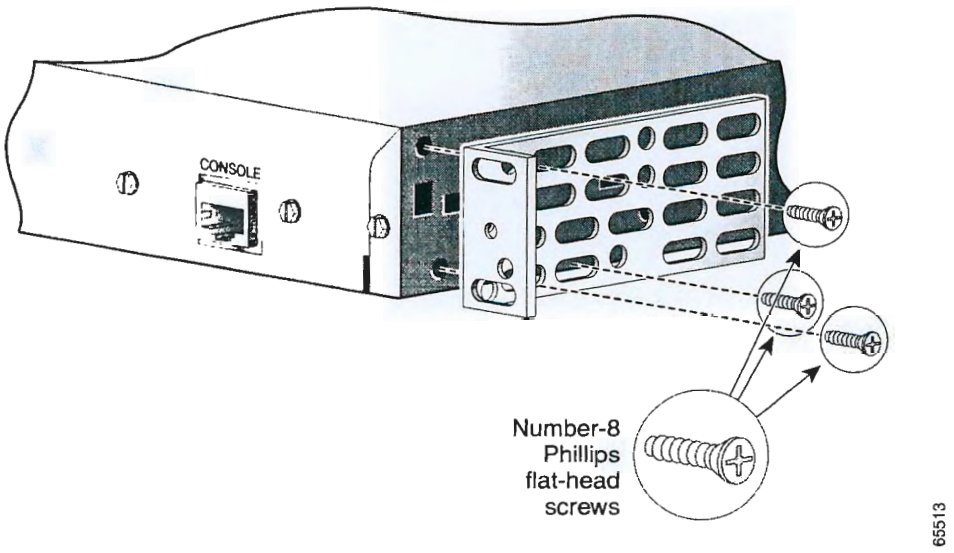
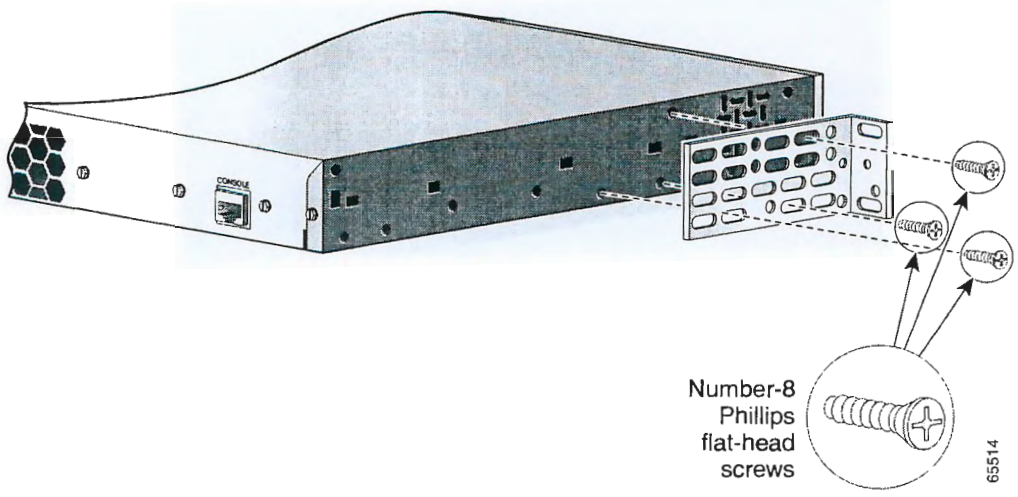


Figure 2-6 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Telco Rack



ROS nº 03/2005 - CN
CPMI - CORREIOS
0092
Fls. Nº
3690
Doc.

Figure 2-7 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack (Front Panel Forward)

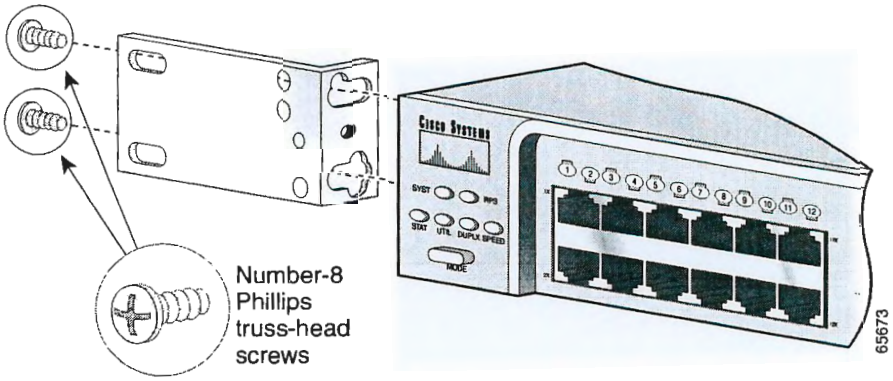
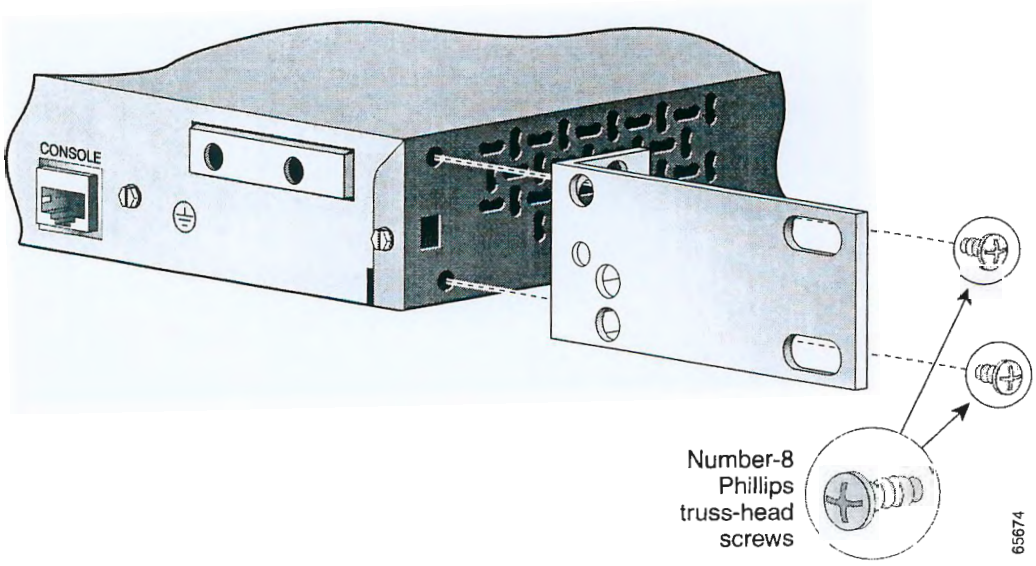


Figure 2-8 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack (Rear Panel Forward)



RQS nº 03/2005 - CN
CPMI - CORREIOS
0833
Fls. Nº
3690
Doc.

Figure 2-9 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack

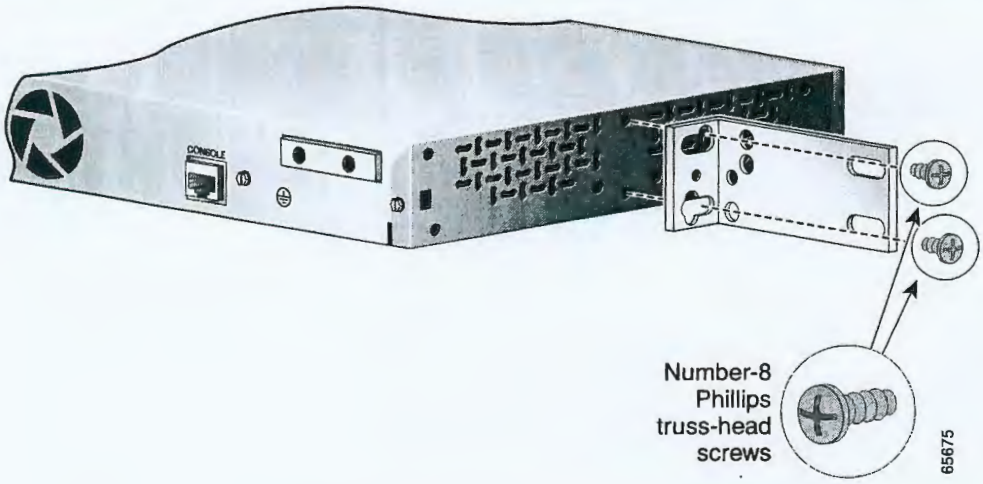
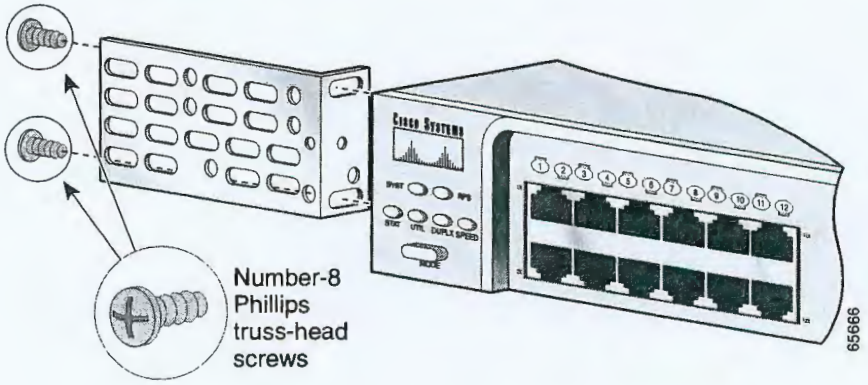
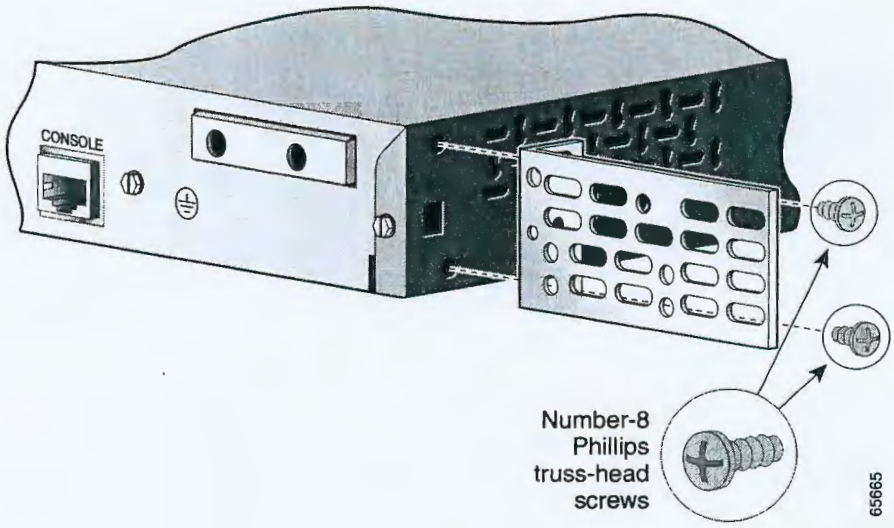


Figure 2-10 Attaching Brackets on the Switch in a 24-Inch Rack (Front Panel Forward)



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0834
3690
Doc.

Figure 2-11 Attaching Brackets on the Switch in a 24-Inch Rack (Rear Panel Forward)



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0835
Doc. 3690

Figure 2-12 Attaching Brackets on the Switch in a 24-Inch Telco Rack

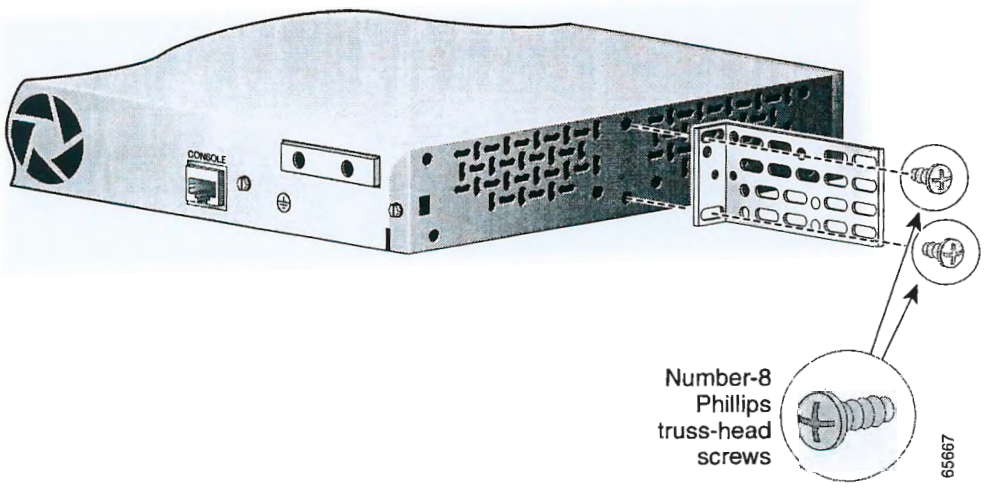
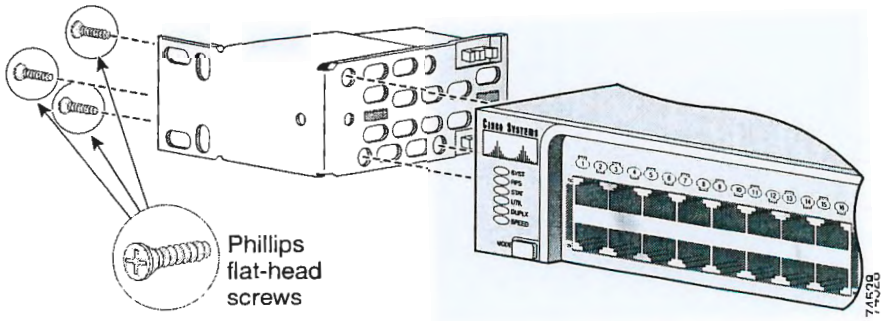


Figure 2-13 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Front Panel Forward)



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0836
Doc. 3690

Figure 2-14 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Rear Panel Forward)

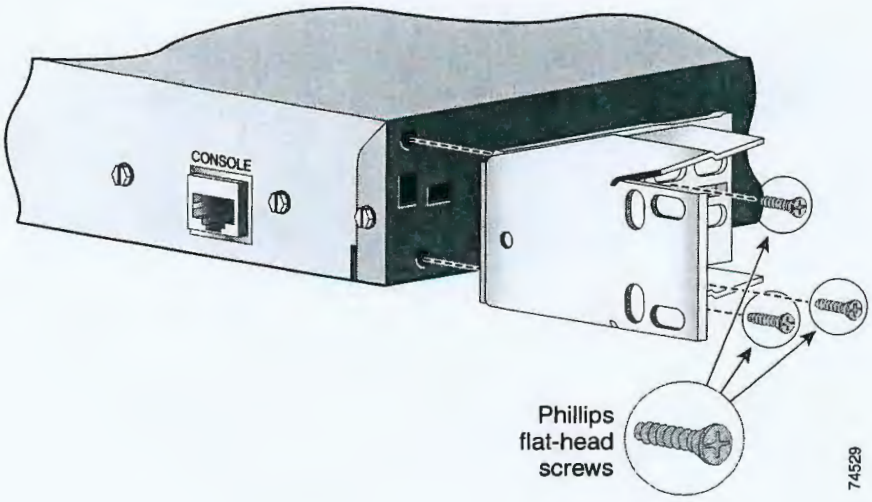
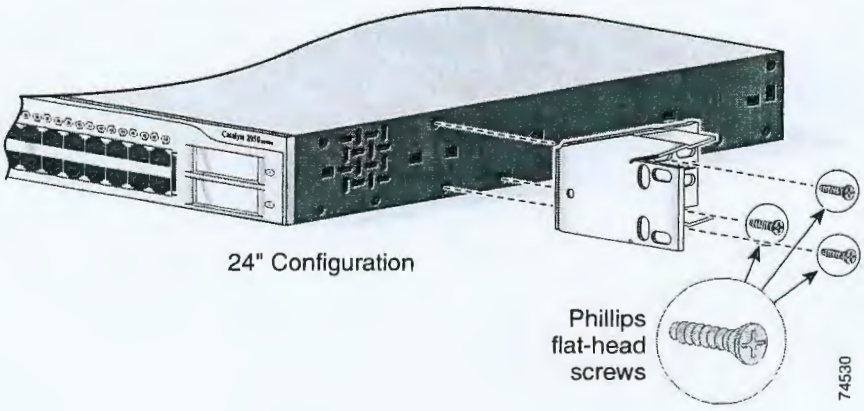


Figure 2-15 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Telco Rack



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0837
Doc. 3690

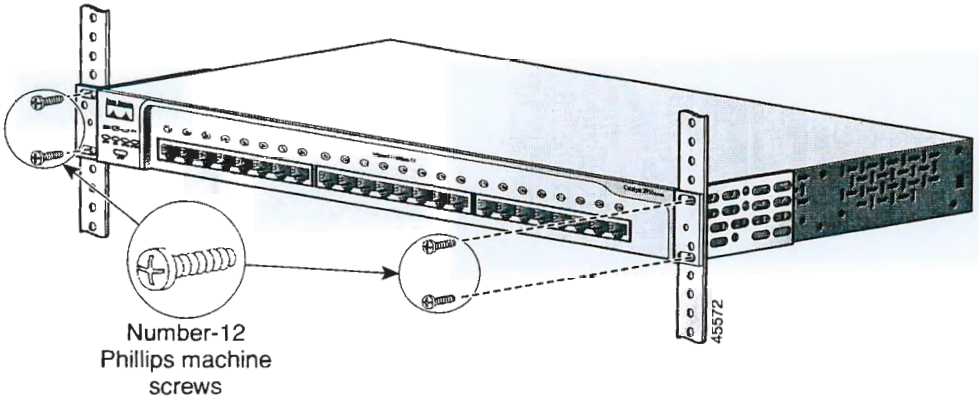
15.027
A

Mounting the Switch in a Rack

After attaching the brackets, use the four Phillips machine screws to securely attach the brackets to the rack, as shown in Figure 2-16.

To prevent the cables from obscuring the switch and other devices in the rack, you can also attach the cable guide to the rack. See the"Attaching the Optional Cable Guide" section for instructions.

Figure 2-16 Mounting the Switch in a Rack



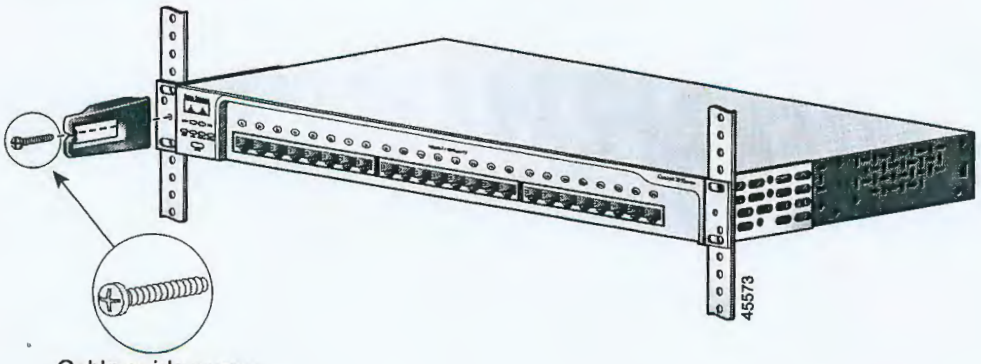
After mounting the switch in the rack, start the terminal-emulation software, and provide power to the switch. See the "Powering On the Switch" section on page 2-22 for instructions.

Attaching the Optional Cable Guide

We recommend attaching the cable guide to prevent the cables from obscuring the front panels of the switch and other devices installed in the rack. Use the supplied black Phillips machine screw to attach the cable guide to the left or right bracket, as shown in Figure 2-17.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0838
Doc. 3690

Figure 2-17 Attaching the Cable Guide



Installing the Switch on a Table, Shelf, or Desk

Before placing the switch on a table, shelf, or desk, locate the adhesive strip with rubber feet in the mounting-kit envelope, and attach four rubber feet to the recessed areas on the switch bottom. Place the switch on a table, shelf, or desk near an AC power source or DC-input power source.

Start the terminal-emulation software and provide power to the switch. See the "Powering On the Switch" section for instructions.

Installing the GBIC Modules

Figure 2-18, Figure 2-19, and Figure 2-20 show how to insert a GBIC module in a GBIC module slot on the switch. For instructions about how to install a CWDM GBIC module in a GBIC module slot, refer to the documentation that came with that GBIC module.

For detailed instructions on installing, removing, and cabling the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to your GBIC documentation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0839
Doc. 3690

Caution To prevent electrostatic-discharge (ESD) damage when installing GBIC modules, follow your normal board and component handling procedures.

Figure 2-18 Installing a 1000BASE-X GBIC Module in a Switch

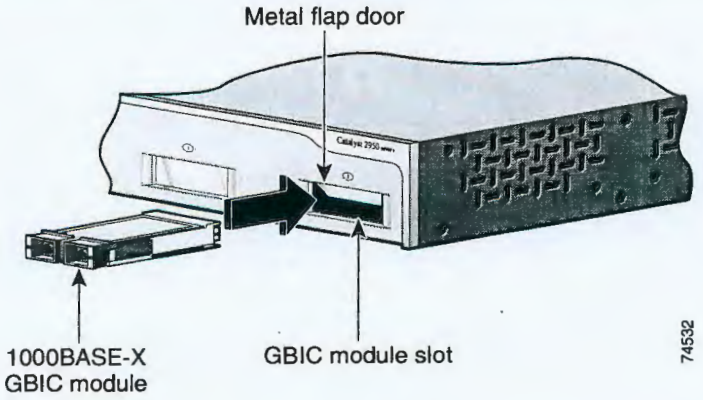
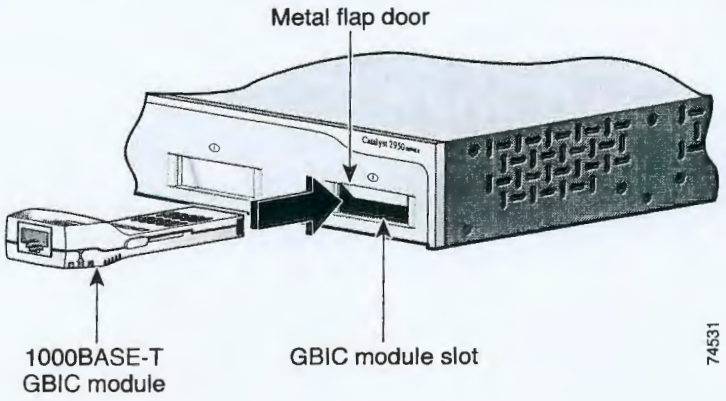
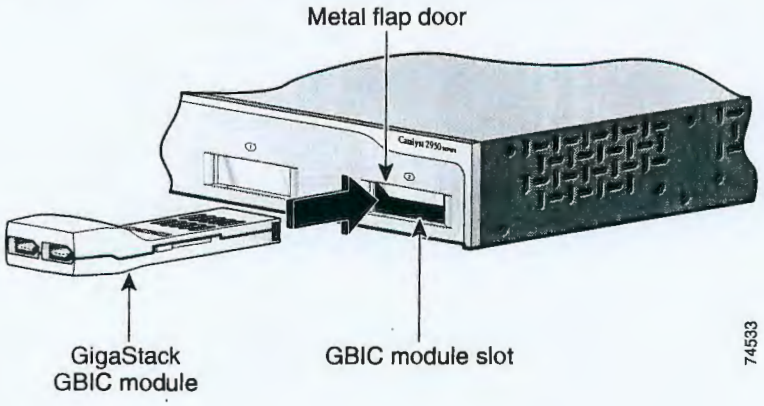


Figure 2-19 Installing a 1000BASE-T GBIC Module in a Switch



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0840
Doc. 3690

Figure 2-20 Installing a GigaStack GBIC Module in a Switch



Powering On the Switch

Before connecting the AC power cord, a DC-input power source, or the Redundant Power System (RPS) to the switch, make sure that you have started the terminal-emulation software (such as ProComm, HyperTerminal, tip, or minicom) from your management station.

If you are using the AC power cord, connect the AC power cord to the AC power connector and to an AC power outlet.

If you are using the DC-input power source, see the "Connecting to DC Power" section for installation instructions.

If you are using an RPS, refer to the documentation that came with your RPS for installation instructions.

Warning **Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle.**

For POST information, see the "Running POST" section on page 2-32.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0841
Doc. 3690

Connecting to DC Power

To connect the Catalyst 2950G-24-EI-DC switch to a DC-input power source, follow these steps:

- Preparing for Installation, page 2-23
- Grounding the Switch, page 2-24
- Wiring the DC-Input Power Source, page 2-26

Warning **The Catalyst 2950G-24-EI-DC contains no field-replaceable units (FRUs). Do not open the chassis or attempt to remove or replace any components. For information about obtaining service for this unit, contact your reseller or Cisco sales representative.**

Warning **The equipment is to be installed in a restricted access area.**

Warning **Ethernet cables must be shielded when used in a central office environment.**

Preparing for Installation

Locate the DC terminal block plug, the ground lug, and the two number-10-32 screws in the DC-switch kit.

Obtain these necessary tools and equipment:

- Ratcheting torque screwdriver with a Phillips head that exerts up to 15 pound-force inches (lbf-in.) of pressure
- Panduit crimping tool with optional controlled cycle mechanism (model CT-700, CT-720, CT-920, CT-920CH, CT-930, or CT-940CH)
- 6-gauge copper ground wire (insulated or noninsulated)
- Four leads of 18-gauge copper wire
- Wire-stripping tools for stripping 6- and 18-gauge wires

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0842
Doc. 3690

Grounding the Switch

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

Warning **When installing the unit, always make the ground connection first and disconnect it last.**

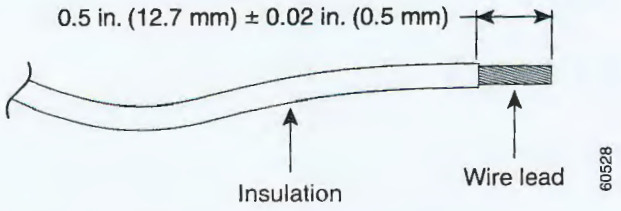
Caution To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions, and use a UL-listed lug suitable for number-6 AWG wire and two number-10-32 ground-lug screws.

To ground the switch to earth ground, follow these steps. Make sure to follow any grounding requirements at your site.

Step 1 Locate the ground lug and the two number-10-32 screws from the switch rear panel. Use a standard Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head. Set the screws and the ground lug aside.

Step 2 If your ground wire is insulated, use a wire stripping tool to strip the 6-gauge ground wire to 0.5 inch (12.7 millimeter [mm]) 0.02 inch (0.5 mm) as shown in Figure 2-21.

Figure 2-21 Stripping the Ground Wire



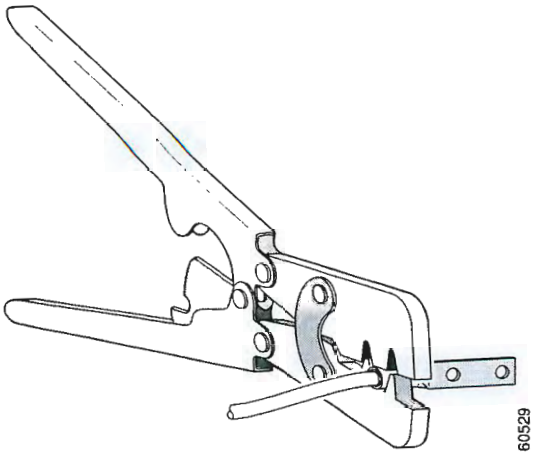
Step 3 Slide the open end of the ground lug over the exposed area of the 6-gauge wire.

RQS nº 03/2005 - CN
CPMI - CORREIOS
78-11157-03
Fls. Nº 0843
Doc. 3690

15.021
A

Step 4 Using a Panduit crimping tool, crimp the ground lug to the 6-gauge wire.

Figure 2-22 Crimping the Ground Lug

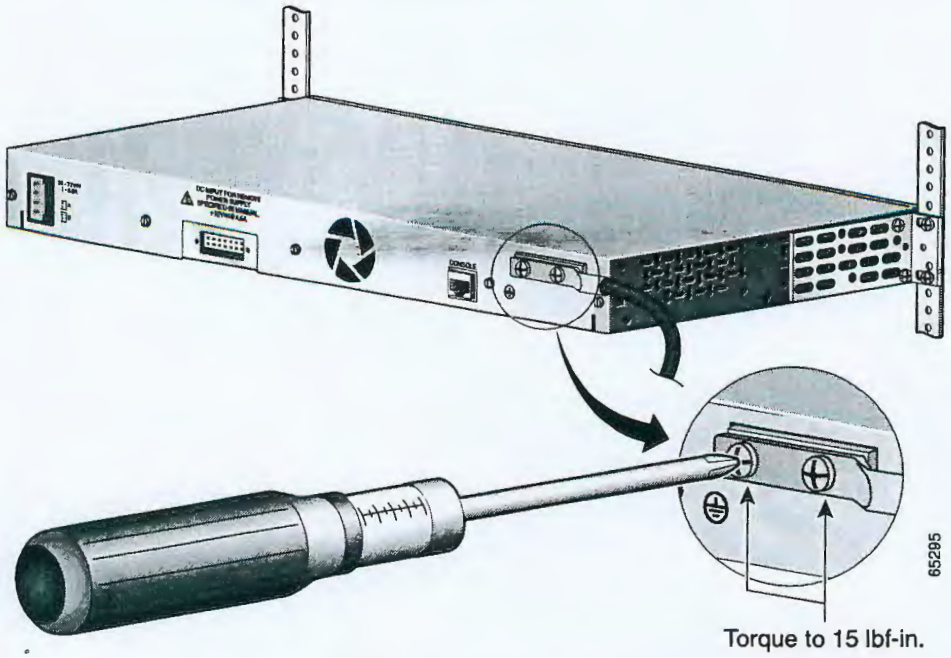


Step 5 Use the two number-10-32 screws to attach the ground lug and wire assembly to the switch rear panel.

Step 6 Using a ratcheting torque screwdriver, torque each ground-lug screw to 15 lbf-in. (240 ounce-force inches [ozf-in.]).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0844
Doc. 3690

Figure 2-23 Torquing Ground-Lug Screws



Wiring the DC-Input Power Source

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0845
Doc. 3690

15.019
A.

Caution You must connect the Catalyst 2950G-24-EI-DC switch only to a DC-input power source that has an input supply voltage from –36 to –72 VDC. If the supply voltage is not in this range, the switch might not operate properly or might be damaged.

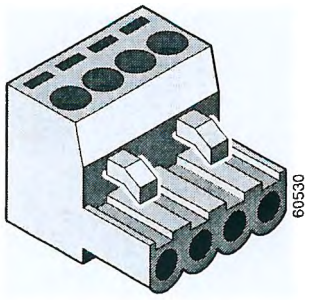
Caution The switch must be installed with 5A-branch-circuit protection.

Note This installation must comply with all applicable codes.

To wire the switch to a DC-input power source, follow these steps:

Step 1 Locate the terminal block plug (see Figure 2-24).

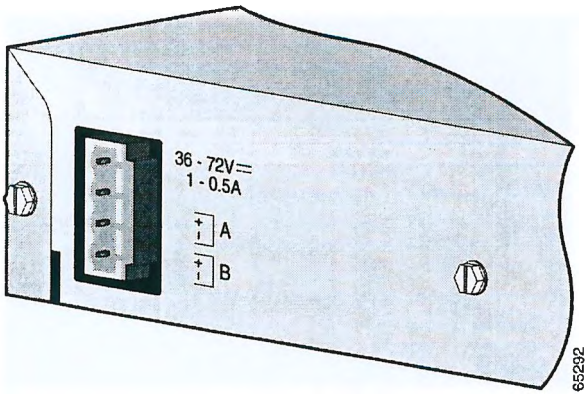
Figure 2-24 Terminal Block Plug



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0846
Doc. 3690

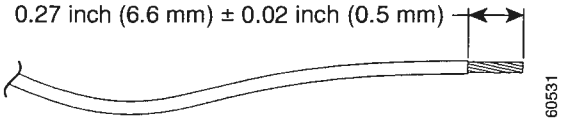
Step 2 Identify the positive and negative feed positions for the terminal block connection. The wiring sequence is positive to positive and negative to negative for both the A and the B feed wires. The switch rear panel identifies the positive and negative positions for both the A and B feed wires.

Figure 2-25 Positive and Negative Positions on the Switch Rear Panel



Step 3 Using an 18-gauge wire-stripping tool, strip each of the four wires coming from the DC-input power source to 0.27 inch (6.6 mm) 0.02 inch (0.5 mm). Do not strip more than 0.29 inch (7.4 mm) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the terminal block plug after installation.

Figure 2-26 Stripping the DC-Input Power Source Wire



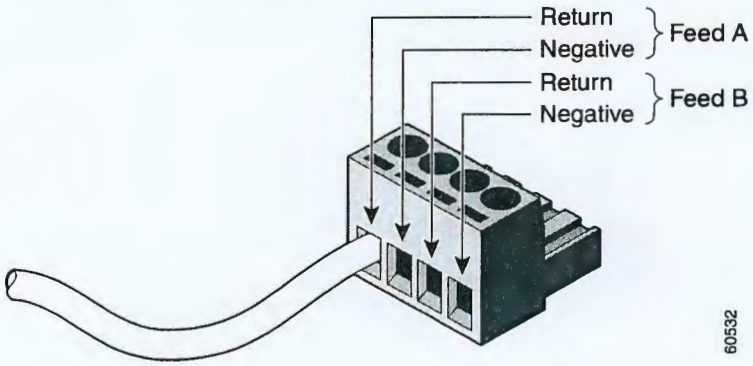
Step 4 Insert the exposed wire of one of the four DC-input power source wires into the terminal block plug, as shown in Figure 2-27. Make sure that you cannot see any wire lead. Only wire *with insulation* should extend from the terminal block.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0847
Doc. 3690

15.017
A.

Warning **An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.**

Figure 2-27 Inserting Wires in the Terminal Block Plug



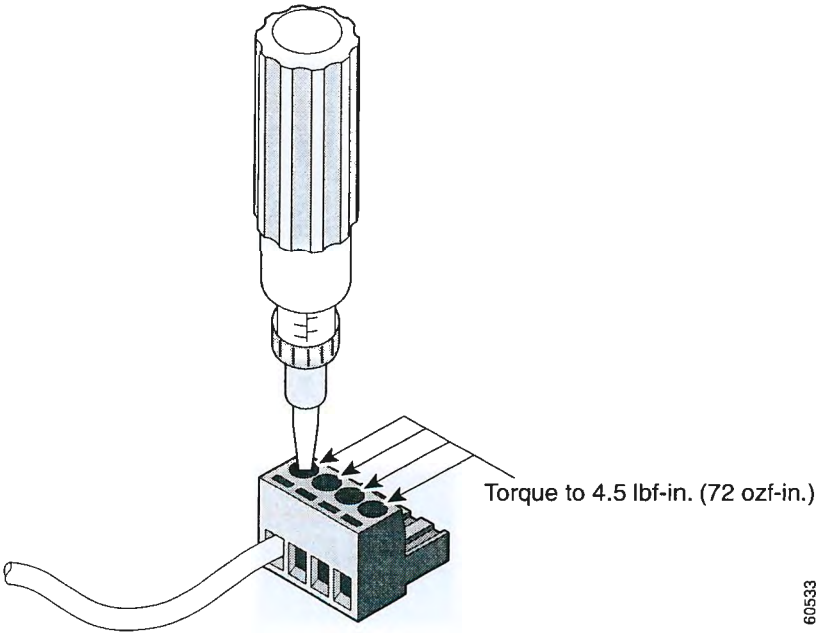
Step 5 Use a ratcheting torque screwdriver to torque the terminal block captive screw (above the installed wire lead) to 4.5 lbf-in. (72 ozf-in.). (See Figure 2-28.)

Caution Do not overtorque the terminal-block captive screws. The recommended maximum torque is 4.5 lbf-in.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0848
Doc. 3690

15.010
A.

Figure 2-28 Torquing the Terminal-Block Captive Screws

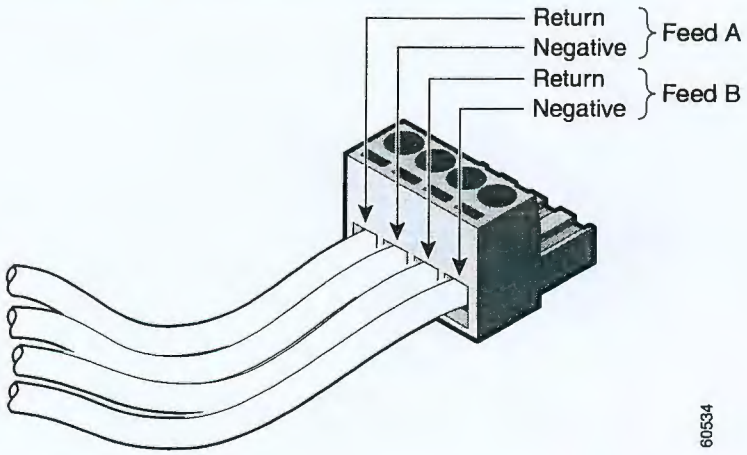


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0849
Doc. 3690

15.015
A-

Step 6 Repeat Steps 4 and 5 for the remaining three DC-input power source wires. Figure 2-29 shows the completed wiring of a terminal block plug.

Figure 2-29 Completed Wiring of Terminal Block Plug

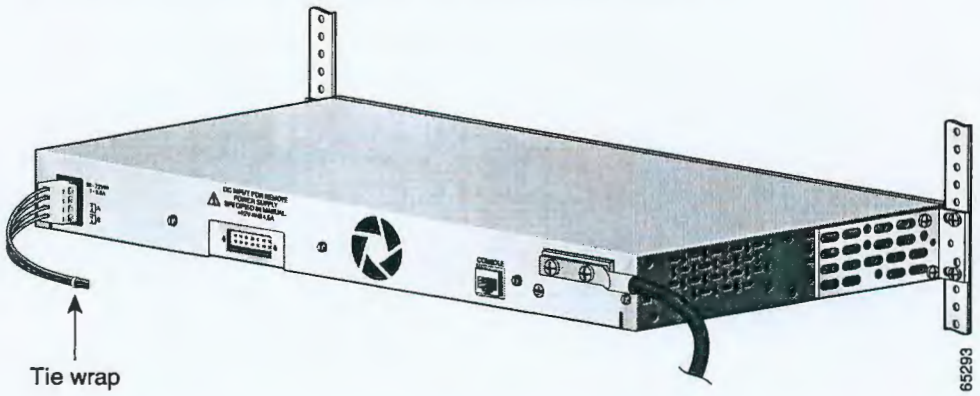


Step 7 Insert the terminal block plug in the terminal block header on the switch rear panel (see Figure 2-30).

Caution Secure the wires coming in from the terminal block so that they cannot be disturbed by casual contact. For example, use tie wraps to secure the wires to the rack.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0850
Doc. 3690

Figure 2-30 Inserting the Terminal Block in the Block Header



Step 8 Remove the tape from the circuit-breaker switch handle, and move the circuit-breaker handle to the on position.

Running POST

After the power is connected, the switch automatically begins POST, a series of tests that verifies that the switch functions properly. When the switch begins POST, the system LED is off. If POST completes successfully, the LED turns green. If POST fails, the LED turns amber. See Chapter 3, "Troubleshooting," to determine a corrective action.

Note POST failures are usually fatal. Call Cisco Systems immediately if your switch does not pass POST.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0851
Doc. 3690

15.013
A.

Connecting to 10/100 and 10/100/1000 Ports

The 10/100 ports configure themselves to operate at the speed and duplex settings of attached devices.They operate at 10 or 100 Mbps in half- or full-duplex mode. If the attached devices do not support autonegotiation, you can explicitly set the speed and duplex parameters.

The 10/100/1000 ports configure themselves to operate at the speed setting of attached devices.These ports on Catalyst 2950T-24 switches operate at 10, 100, or 1000 Mbps only in full-duplex mode. If the attached devices do not support autonegotiation, you can explicitly set the speed parameter.

Connecting devices that do not autonegotiate or devices with manually set speed and duplex parameters can reduce performance or result in link failures between the devices. To maximize performance, choose one of these methods for configuring the ports:

- Let the ports autonegotiate both speed and duplex for 10/100 ports and only speed for 10/100/1000 ports.
- Set the speed and duplex parameters on both ends of the connection.

When connecting the ports on the Catalyst 2950G-24-EI-DC switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC switch is suitable only for intrabuilding or nonexposed wiring connections.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0852
Doc. 3690

15.012
A.

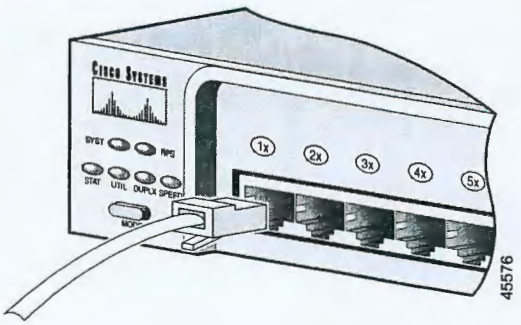
Follow these steps to connect the switch to 10BASE-T, 100BASE-TX, or 1000BASE-T devices:

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a twisted-pair straight-through cable in a front-panel RJ-45 connector, as shown in Figure 2-31, Figure 2-32, and Figure 2-33. When connecting to switches or repeaters, insert a twisted-pair crossover cable. (See the "Cable and Adapter Specifications" section on page B-7 for cable-pinout descriptions.)

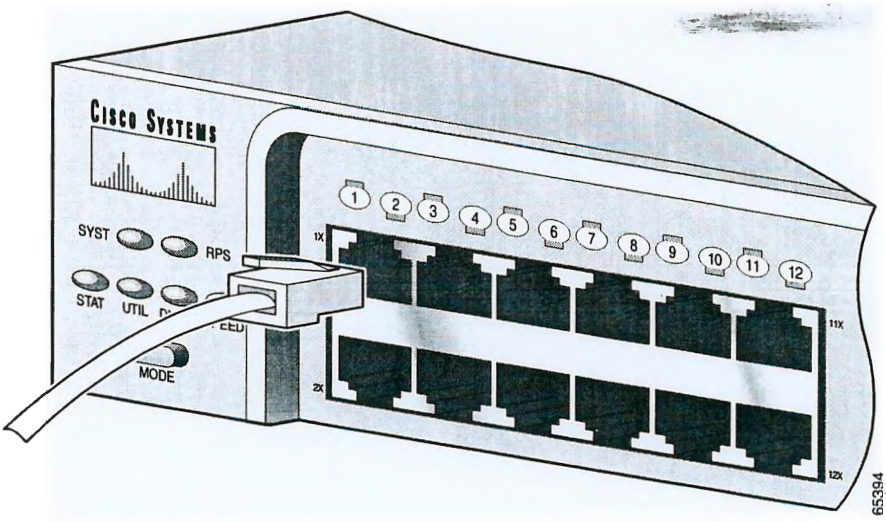
Note When connecting to 1000BASE-T devices, be sure to use a four twisted-pair, Category 5 cable.

Figure 2-31 Connecting to a Port on Catalyst 2950-12, 2950-24, 2950C-24, 2950SX-24, and 2950T-24 Switches



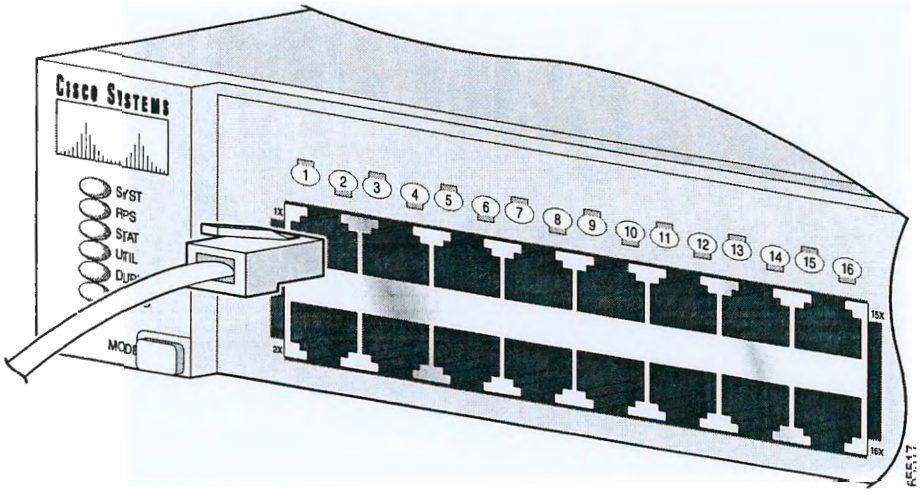
78-11157-03
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0853
Doc. 3690

Figure 2-32 Connecting to a Port on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches



RQS.nº 03/2005 - CN
CPMI CORREIOS
0854
Fls. Nº
3690
Doc.

Figure 2-33 Connecting to a Port on Catalyst 2950G-48-EI Switches



Step 2 Insert the other cable end in an RJ-45 connector on the target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while Spanning Tree Protocol (STP) discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the target device if necessary.

Step 5 Repeat Steps 1 through 4 to connect each port.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0855
Doc. 3690

15.009
A.

Connecting to 100BASE-FX and 1000BASE-SX Ports

The 100BASE-FX and 1000BASE-SX ports operate only in full-duplex mode.

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on another device by using one of the MT-RJ fiber-optic patch cables listed in Table 2-1. Use the Cisco part numbers in Table 2-1 to order the patch cables that you need.

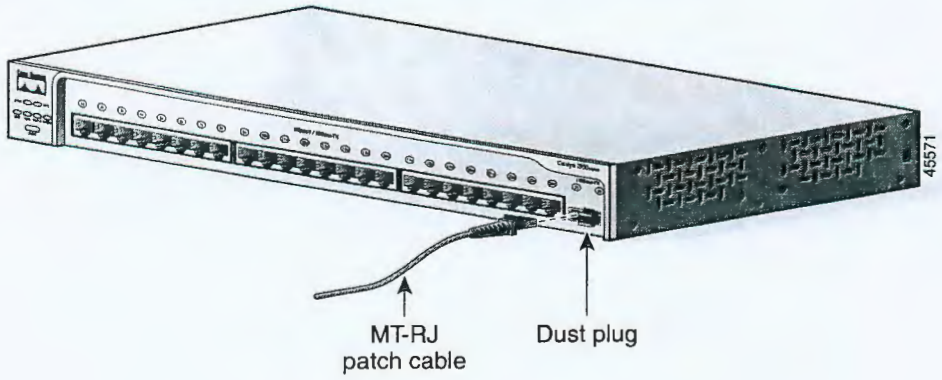
Follow these steps to connect the switch to a 100BASE-FX or 1000BASE-SX device:

Caution Do not remove the dust plugs from the fiber-optic ports or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the fiber-optic ports and cables from contamination and ambient light.

Step 1 Remove the dust plugs from the 100BASE-FX or 1000BASE-SX port and the rubber caps from the MT-RJ patch cable. Store them for future use.

Step 2 Insert the cable in a 100BASE-FX or 1000BASE-SX port. (See Figure 2-34.)

Figure 2-34 Connecting to a 100BASE-FX or 1000BASE-SX Port



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0856
3690
Doc.

15003
SA.

Step 3 Insert the other cable end in an SC or ST port on the target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the target device if necessary.

Step 6 Repeat Steps 1 through 5 to connect each port.

Connecting to GBIC Module Ports

These sections describe how to connect to a GBIC module port.

- Connecting to 1000BASE-X GBIC Module Ports, page 2-39
- Connecting to 1000BASE-T GBIC Module Ports, page 2-41
- Connecting to GigaStack GBIC Module Ports, page 2-42

For instructions about how to connect to the CWDM GBIC module ports, refer to the documentation that came with that GBIC module.

For detailed instructions about installing, removing, and connecting to the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to the GBIC documentation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0857
3690
Doc.

When connecting the ports on the Catalyst 2950G-24-EI-DC switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC switch is suitable only for intrabuilding or nonexposed wiring connections.

Connecting to 1000BASE-X GBIC Module Ports

Caution Do not remove the rubber plugs from the GBIC module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the GBIC module ports and cables from contamination and ambient light.

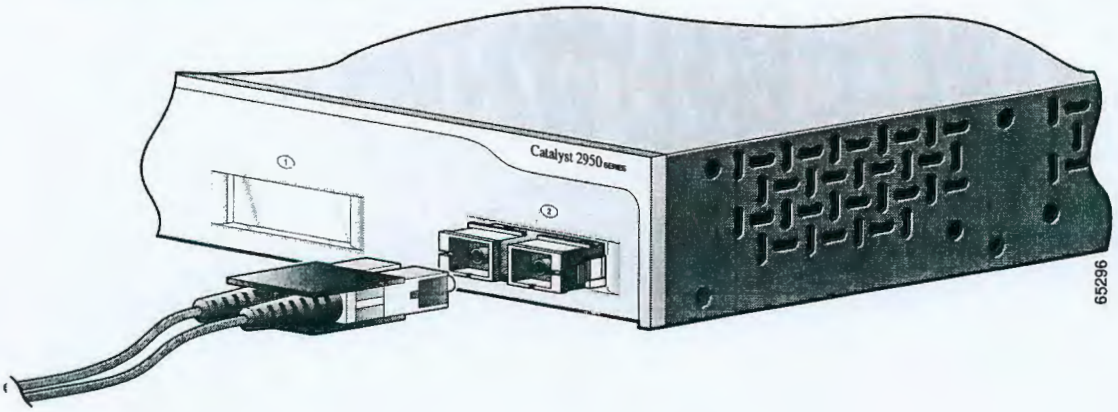
After installing the 1000BASE-X GBIC in the GBIC module slot, follow these steps:

Step 1 Remove the rubber plugs from the GBIC module port, and store them for future use.

Step 2 Insert the SC connector in the fiber-optic receptacle (see Figure 2-35).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0858
Doc. 3690

Figure 2-35 Connecting to a 1000 BASE-X GBIC Port



Step 3 Insert the other cable end in a fiber-optic receptacle on a target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the switch or target device if necessary.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0859
Doc. 3690

15005
A-

Connecting to 1000BASE-T GBIC Module Ports

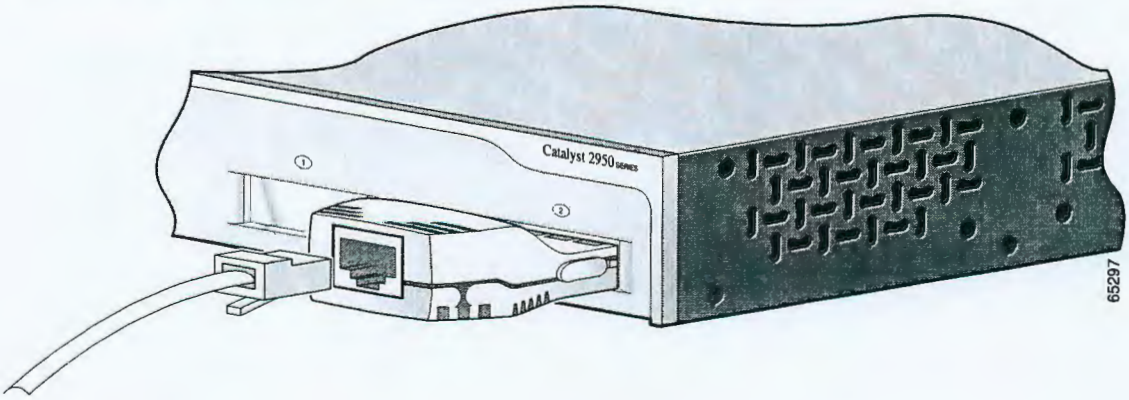
After installing the 1000BASE-T GBIC in the GBIC module slot, follow these steps:

Caution To prevent ESD damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a four twisted-pair, straight-through cable in the RJ-45 connector. When connecting to switches or repeaters, insert a four twisted-pair, crossover cable (see Figure 2-36).

Note When connecting to a 1000BASE-T device, be sure to use a four twisted-pair, Category 5 cable.

Figure 2-36 Connecting to a 1000BASE-T GBIC Port



Step 2 Insert the other cable end in an RJ-45 connector on a target device.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0860
Doc. 3690

15.004
CA.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

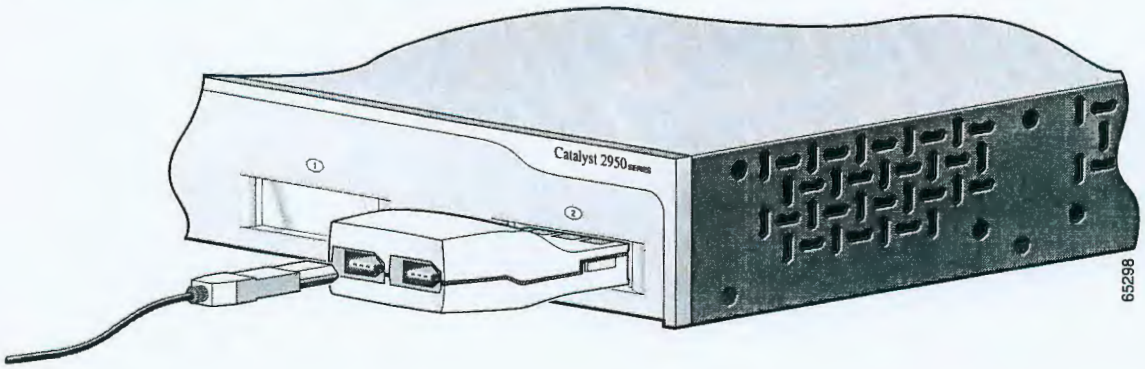
Step 4 Reconfigure and restart the switch or target device, if necessary.

Connecting to GigaStack GBIC Module Ports

After installing the GigaStack GBIC in the GBIC module slot, follow these steps:

Step 1 Insert the GigaStack cable connector in the GBIC (see Figure 2-37).

Figure 2-37 Connecting to a GigaStack GBIC Port



Step 2 Insert the other cable end in a port on a target device.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0861
3690
Doc.

15.003
64

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the switch or target device, if necessary.

Connecting a PC or a Terminal to the Console Port

If you want to connect a PC to the console port, use the supplied RJ-45-to-DB-9 adapter cable. If you want to connect a terminal to the console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco. For console-port and adapter-pinout information, see the"Cable and Adapter Specifications" section on page B-7.

The PC or terminal must support VT100 terminal emulation. The terminal-emulation software—frequently a PC application such as HyperTerminal or Procomm Plus—makes communication between the switch and your PC or terminal possible during the setup program.

Follow these steps to connect your PC or terminal to the console port:

Step 1 Make sure that your terminal-emulation software is configured to communicate with the switch through hardware flow control.

Step 2 Configure the baud rate and character format of the PC or terminal to match these console-port default characteristics:

- 9600 baud
- Eight data bits
- One stop bit
- No parity

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0862
3690
Doc.

15.002
LA.

After gaining access to the switch, you can change the port baud rate. Refer to the switch software configuration guide for instructions.

Step 3 Insert the adapter cable in the console port, as shown in Figure 2-38, Figure 2-39, and Figure 2-40. (See the "Cable and Adapter Pinouts" section on page B-10 for pinout descriptions.)

Figure 2-38 Connecting to the Console Port

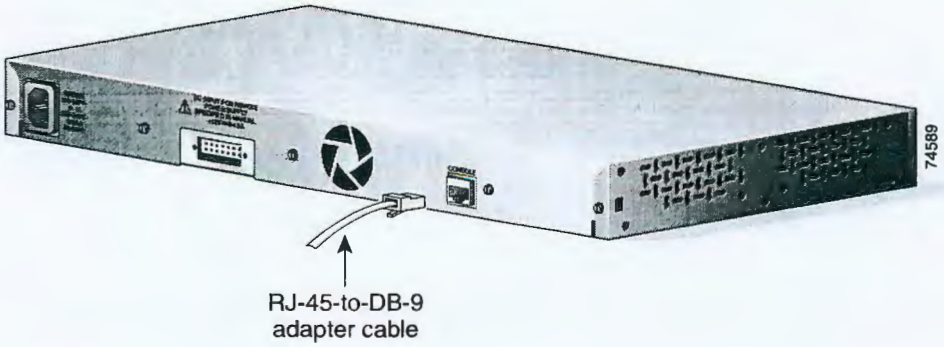
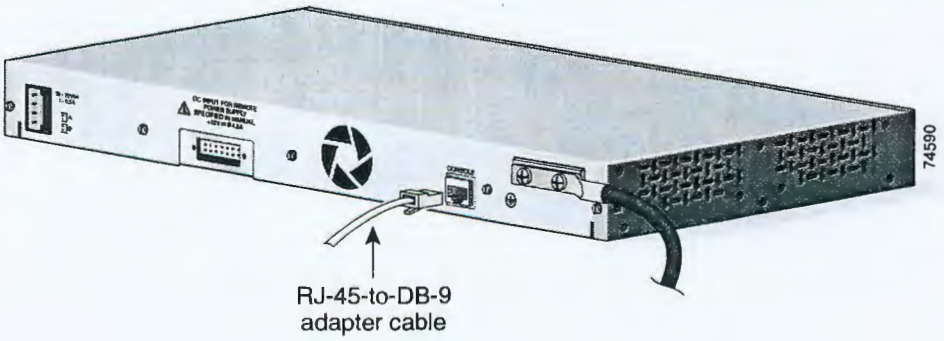
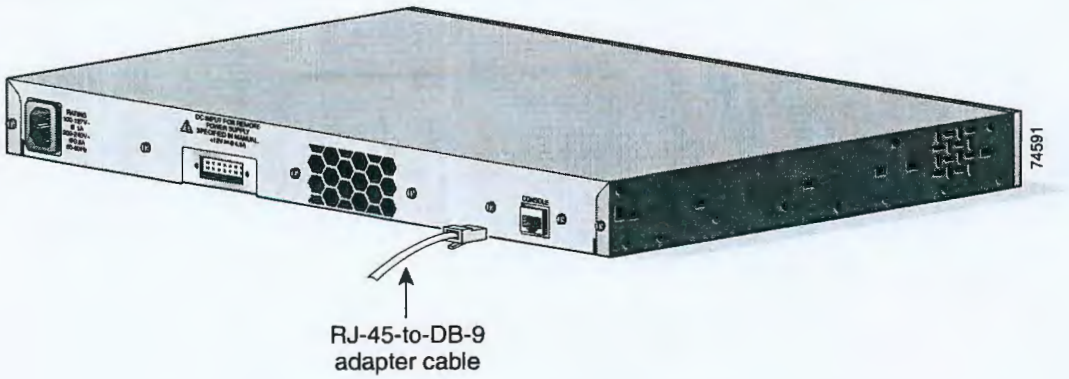


Figure 2-39 Connecting to a Console Port Only on Catalyst 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1863
3690
Doc.

Figure 2-40 Connecting to a Console Port Only on Catalyst 2950G-48-EI Switches



Step 4 Attach the appropriate adapter to the terminal, if needed.

Step 5 Insert the other adapter cable end in the PC or terminal adapter.

Step 6 Start the terminal-emulation software.

Where to Go Next

For information about starting up the switch, refer to the *Release Notes for the Catalyst 2950 Switch.*

For information about configuring the switch, refer to the switch software configuration guide.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0864
Doc. 3690

15.000
V4-

RQS nº 03/2005 - CN
CPMI - CORREIOS
0865
Fls. Nº
Doc. 3690

roriz@IBM-297NYWD11S3

14999
A.

Job Title: SWITCH_TIPO2_doc4.pdf

Time Queued: Thu Jul 24 03:35:13 2003
Time Printed: Thu Jul 24 04:12:34 2003

Submitted By: roriz@IBM-297NYWD11S3

roriz@IBM-297NYWD11S3

Need help? Call your local NCO HelpDesk.

PIO_DEV: ibm@brbrap7a#ibmNetPrinter (ibm4320) @ brbraprt01

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0866
Doc. 3690

CHAPTER 13

Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094). It includes information about VLAN modes and the VLAN Membership Policy Server (VMPS).

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

The chapter includes these sections:

- Understanding VLANs, page 13-1
- Configuring Normal-Range VLANs, page 13-6
- Configuring Extended-Range VLANs, page 13-14
- Displaying VLANs, page 13-16
- Configuring VLAN Trunks, page 13-18
- Configuring VMPS, page 13-30

Understanding VLANs

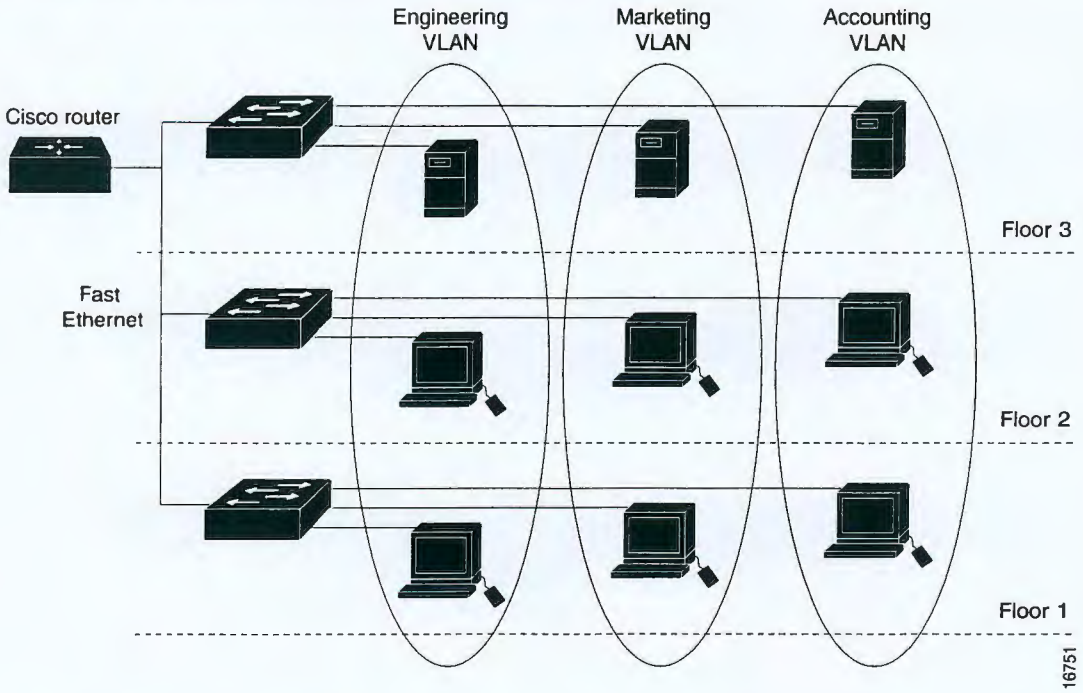
A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge as shown in Figure 13-1. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree. See Chapter 10, "Configuring STP" and Chapter 11, "Configuring RSTP and MSTP."

Note Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network. For more information on VTP, see Chapter 14, "Configuring VTP."

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0867
3690
Doc.

Figure 13-1 shows an example of VLANs segmented into logically defined networks.

Figure 13-1 VLANs as Logically Defined Networks



VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Supported VLANs

Table 13-1 lists the number of supported VLANs on Catalyst 2950 switches.

Table 13-1 Maximum Number of Supported VLANs

Switch Model	Number of Supported VLANs
Catalyst 2950-12	64
Catalyst 2950-24	64
Catalyst 2950C-24	250
Catalyst 2950G-12-EI	250
Catalyst 2950G-24-EI	250
Catalyst 2950G-48-EI	250
Catalyst 2950G-24-EI-DC	250
Catalyst 2950T-24	250

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0868
Doc. 3690

14.996
4

VLANs are identified with a number from 1 to 4094 when the enhanced software image is installed and 1 to 1005 when the standard software image is installed. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VTP only learns normal-range VLANs, with VLAN IDs 1 to 1005; VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database. The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094.

The switch supports per-VLAN spanning tree (PVST) with a maximum of 64 spanning-tree instances. One spanning-tree instance is allowed per VLAN. See the "Configuration Guidelines for Normal-Range VLANs" section on page 13-7 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

Note The Catalyst 2950 switches do not support Inter-Switch Link (ISL) trunking.

Management VLANs

Communication with the switch management interfaces is through the switch IP address. The IP address is associated with the management VLAN, which by default is VLAN 1.

The management VLAN has these characteristics:

- It is created from CMS or through the CLI on static-access, dynamic-access, and trunk ports. You cannot create or remove the management VLAN through Simple Network Management Protocol (SNMP).
- Only one management VLAN can be administratively active at a time.
- With the exception of VLAN 1, the management VLAN can be deleted.
- When created, the management VLAN is administratively down.

Before changing the management VLAN on your switch network, make sure you follow these guidelines:

- The new management VLAN should not have a Hot Standby Router Protocol (HSRP) standby group configured on it.
- You must be able to move your network management station to a switch port assigned to the same VLAN as the new management VLAN.
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.
- On switches running a IOS software version that is earlier than Cisco IOS 12.0(5)XP, you cannot change the management VLAN. Switches running Cisco IOS 12.0(5)XP should be upgraded to the current software release as described in the release notes.

If you are using SNMP or CMS to manage the switch, ensure that the port through which you are connected to a switch is in the management VLAN.

For information about the role management VLANs play in switch clusters, see the "Management VLAN" section on page 6-20.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0869
Doc. 3690

Determining the Management VLAN for a New Switch

If you add a new switch to an existing cluster and the cluster is using a management VLAN other than the default VLAN 1, the command switch automatically senses that the new switch has a different management VLAN and has not been configured. The command switch issues commands to change the management VLAN on the new switch to match the one used by the cluster. This automatic change occurs for new, out-of-box switches that do not have a config.text file and for which there have been no changes to the running configuration.

Before a new switch can be added to a cluster, it must be connected to a port that belongs to the cluster management VLAN. If the cluster is configured with a management VLAN other than the default, the command switch changes the management VLAN for new switches when they are connected to the cluster. In this way, the new switch can exchange Cisco Discovery Protocol (CDP) messages with the command switch and be proposed as a cluster candidate.

Note For the command switch to change the management VLAN on a new switch, there must have been no changes to the new switch configuration, and there must be no config.text file.

Because the switch is new and unconfigured, its management VLAN is changed to the cluster management VLAN when it is first added to the cluster. All ports that have an active link at the time of this change become members of the new management VLAN.

For information about the role management VLANs play in switch clusters, see the "Management VLAN" section on page 6-20.

Changing the Management VLAN for a Cluster

Beginning in privileged EXEC mode on the command switch, follow these steps to configure the management VLAN interface through a Telnet or Secure Shell (SSH) connection:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cluster management-vlan** *vlanid*	Change the management VLAN for the cluster. This ends your Telnet session. Change the port through which you are connected to the switch to a port in the new management VLAN.
Step 3	**show running-config**	Verify the change.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0870
Doc. 3690

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that determines the kind of traffic the port carries and the number of VLANs to which it can belong. Table 13-2 lists the membership modes and membership and VTP characteristics.

Table 13-2 Port Membership Modes

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 13-13.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent to disable VTP. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.
802.1Q trunk	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list. For information about configuring trunk ports, see the "Configuring an Ethernet Interface as a Trunk Port" section on page 13-21.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.
Dynamic access	A dynamic-access port can belong to one normal-range VLAN (VLAN ID 1 to 1005) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6000 series switch, for example, but never a Catalyst 2950 switch. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station and not to another switch. For configuration information, see the "Configuring Dynamic Access Ports on VMPS Clients" section on page 13-34.	VTP is required. Configure the VMPS and the client with the same VTP domain name. You can change the reconfirmation interval and retry count on the VMPS client switch.

For more detailed definitions of the modes and their functions, see Table 13-5 on page 13-20.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the "Managing the MAC Address Table" section on page 7-52.

RQS nº 03/2005 - CN
CPMI – CORREIOS
Fls. Nº 0871
3690
Doc.

Configuring Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. If the switch is in VTP server or transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

Note When the switch is in VTP transparent mode and the enhanced software image is installed, you can also create extended-range VLANs (VLANs with IDs from 1006 to 4094), but these VLANs are not saved in the VLAN database. See the "Configuring Extended-Range VLANs" section on page 13-14.

Configurations for VLAN IDs 1 to 1005 are written to the file *vlan.dat* (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in nonvolatile RAM (NVRAM).

Caution You can cause inconsistency in the VLAN database if you attempt to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the *Catalyst 2950 Desktop Switch Command Reference* for this release. To change the VTP configuration, see Chapter 14, "Configuring VTP."

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

Note This section does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

RQS nº 03/2005 - CN
CPMI -- CORREIOS
Fls. Nº 0872
Doc. 3690

This section includes information about these topics about normal-range VLANs:

- Token Ring VLANs, page 13-7
- Configuration Guidelines for Normal-Range VLANs, page 13-7
- VLAN Configuration Mode Options, page 13-8
- Saving VLAN Configuration, page 13-9
- Default Ethernet VLAN Configuration, page 13-10
- Creating or Modifying an Ethernet VLAN, page 13-10
- Deleting a VLAN, page 13-12
- Assigning Static-Access Ports to a VLAN, page 13-13

Token Ring VLANs

Although the Catalyst 2950 switches do not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running VTP version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, refer to the *Catalyst 5000 Series Software Configuration Guide*.

Configuration Guidelines for Normal-Range VLANs

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- See Table 13-1 for the maximum number of supported VLANs per switch model. On a switch supporting 250 VLANs, if VTP reports that there are 254 active VLANs, four of the active VLANs (1002 to 1005) are reserved for Token Ring and FDDI.
- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- VLAN configuration for VLANs 1 to 1005 are always saved in the VLAN database. If VTP mode is transparent, VTP and VLAN configuration is also saved in the switch running configuration file.
- The switch also supports VLAN IDs 1006 through 4094 in VTP transparent mode (VTP disabled) when the enhanced software image is installed. These are extended-range VLANs and configuration options are limited. Extended-range VLANs are not saved in the VLAN database. See the "Configuring Extended-Range VLANs" section on page 13-14.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
- Catalyst 2950 switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The switch supports 64 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 64 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0879
Doc. 3690

running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch exceeds 64, we recommend that you configure the IEEE 802.1S Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 11, "Configuring RSTP and MSTP."

VLAN Configuration Mode Options

You can configure normal-range VLANs (with VLAN IDs 1 to 1005) by using these two configuration modes:

- VLAN Configuration in config-vlan Mode, page 13-8

  You access config-vlan mode by entering the **vlan** *vlan-id* global configuration command.

- VLAN Configuration in VLAN Configuration Mode, page 13-8

  You access VLAN configuration mode by entering the **vlan database** privileged EXEC command.

VLAN Configuration in config-vlan Mode

To access config-vlan mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN or with an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 13-3) or enter multiple commands to configure the VLAN. For more information about commands available in this mode, refer to the **vlan** global configuration command description in the *Catalyst 2950 Desktop Switch Command Reference* for this release. When you have finished the configuration, you must exit config-vlan mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

You must use this config-vlan mode when creating extended-range VLANs (VLAN IDs greater than 1005). See the "Configuring Extended-Range VLANs" section on page 13-14.

VLAN Configuration in VLAN Configuration Mode

To access VLAN configuration mode, enter the **vlan database** privileged EXEC command. Then enter the **vlan** command with a new VLAN ID to create a VLAN or with an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 13-3) or enter multiple commands to configure the VLAN. For more information about keywords available in this mode, refer to the **vlan** VLAN configuration command description in the *Catalyst 2950 Desktop Switch Command Reference* for this release. When you have finished the configuration, you must enter **apply** or **exit** for the configuration to take effect. When you enter the **exit** command, it applies all commands and updates the VLAN database. VTP messages are sent to other switches in the VTP domain, and the privileged EXEC mode prompt appears.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0874
3690
Doc.

Saving VLAN Configuration

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file). If VTP mode is transparent, they are also saved in the switch running configuration file and you can enter the **copy running-config startup-config** privileged EXEC command to save the configuration in the startup configuration file. You can use the **show running-config vlan** privileged EXEC command to display the switch running configuration file. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is determined as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.
- If VTP mode is server, the domain name and VLAN configuration for the first 1005 VLANs use the VLAN database information
- If the switch is running IOS release 12.1(9)EA1 or later and you use an older startup configuration file to boot up the switch, the configuration file does not contain VTP or VLAN information, and the switch uses the VLAN database configurations.
- If the switch is running an IOS release earlier than 12.1(9)EA1 and you use a startup configuration file from IOS release 12.1(9)EA1 or later to boot up the switch, the image on the switch does not recognize the VLAN and VTP configurations in the startup configuration file, so the switch uses the VLAN database configuration.

Caution If the startup configuration file contains extended-range VLAN configuration, this information will be lost when the system boots up.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0875
3690
Doc.

Default Ethernet VLAN Configuration

Table 13-3 shows the default configuration for Ethernet VLANs.

Note The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

Table 13-3 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094 when the enhanced software image is installed and 1 to 1005 when the standard software image is installed. **Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	*VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number	No range
802.10 SAID	100001 (100000 plus the VLAN ID)	1–4294967294
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Creating or Modifying an Ethernet VLAN

Each Ethernet VLAN in the VLAN database has a unique, 4-digit ID that can be a number from 1 to 1001. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs. To create a normal-range VLAN to be added to the VLAN database, assign a number and name to the VLAN.

Note When the switch is in VTP transparent mode and the enhanced software image is installed, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database. See the "Configuring Extended-Range VLANs" section on page 13-14.

For the list of default parameters that are assigned when you add a VLAN, see the "Configuring Normal-Range VLANs" section on page 13-6.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0870
Fls. Nº
3690
Doc.

Beginning in privileged EXEC mode, follow these steps to use config-vlan mode to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter config-vlan mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify a VLAN. **Note** The available VLAN ID range for this command is 1 to 1005 when the standard software image is installed and 1 to 4094 when the enhanced software image is installed; do not enter leading zeros. For information about adding VLAN IDs greater than 1005 (extended-range VLANs), see the "Configuring Extended-Range VLANs" section on page 13-14.
Step 3	**name** *vlan-name*	(Optional) Enter a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size (or other VLAN characteristic).
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries.
Step 7	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To return the VLAN name to the default settings, use the **no vlan name** or **no vlan mtu** config-vlan commands.

This example shows how to use config-vlan mode to create Ethernet VLAN 20, name it *test20,* and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

Beginning in privileged EXEC mode, follow these steps to use VLAN configuration mode to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**vlan** *vlan-id* **name** *vlan-name*	Add an Ethernet VLAN by assigning a number to it. The range is 1 to 1001; do not enter leading zeros. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 3	**vlan** *vlan-id* **mtu** *mtu-size*	(Optional) To modify a VLAN, identify the VLAN and change a characteristic, such as the MTU size.

CPMI - CORREIOS
Fls. Nº 0367
3690
Doc.

	Command	Purpose
Step 4	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 5	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries.
Step 6	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To return the VLAN name to the default settings, use the **no vlan** *vlan-id* **name** or **no vlan** *vlan-id* **mtu** VLAN configuration command.

This example shows how to use VLAN configuration mode to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# vlan database
Switch(vlan)# vlan 20 name test20
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

Deleting a VLAN

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch by using global configuration mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no vlan** *vlan-id*	Remove the VLAN by entering the VLAN ID.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vlan brief**	Verify the VLAN removal.
Step 5	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To delete a VLAN by using VLAN configuration mode, use the **vlan database** privileged EXEC command to enter VLAN configuration mode and the **no vlan** *vlan-id* VLAN configuration command.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 0878
3690
Doc.

14.986
A.

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information (VTP is disabled). If you are assigning a port on a cluster member switch to a VLAN, first use the **rcommand** privileged EXEC command to log in to the member switch.

Note If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 13-10.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**interface** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094; do not enter leading zeros.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.
Step 7	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

This example shows how to configure Fast Ethernet interface 0/1 as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
Switch#
```

These examples show how to verify the configuration:

```
Switch# show running-config interface fastethernet0/1
Building configuration...

Current configuration : 74 bytes
!
interface FastEthernet0/12
 switchport access vlan 2
 switchport mode access
end
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0879
Doc. 3690

```
Switch# show interfaces fastethernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (VLAN0002)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Voice VLAN: none (Inactive)
Appliance trust: none
```

Configuring Extended-Range VLANs

When the switch is in VTP transparent mode (VTP disabled) and the enhanced software image is installed), you can create extended-range VLANs (in the range 1006 to 4094). Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any switchport commands that allow VLAN IDs. You always use config-vlan mode (accessed by entering the **vlan** *vlan-id* global configuration command) to configure extended-range VLANs. The extended range is not supported in VLAN configuration mode (accessed by entering the **vlan database** privileged EXEC command).

Extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Although the switch supports 4094 VLAN IDs when the enhanced software image is installed, see the "Supported VLANs" section on page 13-2 for the actual number of VLANs supported.

This section includes this information about extended-range VLANs:

- Default VLAN Configuration, page 13-14
- Configuration Guidelines for Extended-Range VLANs, page 13-15
- Creating an Extended-Range VLAN, page 13-15
- Displaying VLANs, page 13-16

Default VLAN Configuration

See Table 13-3 on page 13-10 for the default configuration for Ethernet VLANs. You can change only the MTU size on extended-range VLANs; all other characteristics must remain at the default state.

ECT 05/2005 - CN
CPMI - CORREIOS
0880
Fls. Nº
Doc. 3690

14.985
JA

Configuration Guidelines for Extended-Range VLANs

Follow these guidelines when creating extended-range VLANs:

- To add an extended-range VLAN, you must use the **vlan** *vlan-id* global configuration command and access config-vlan mode. You cannot add extended-range VLANs in VLAN configuration mode (accessed by entering the **vlan database** privileged EXEC command).
- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP.
- You cannot include extended-range VLANs in the pruning eligible range.
- The switch must be in VTP transparent mode when you create extended-range VLANs. If VTP mode is server or client, an error message is generated, and the extended-range VLAN is rejected.
- You can set the VTP mode to transparent in global configuration mode or in VLAN configuration mode. See the "Disabling VTP (VTP Transparent Mode)" section on page 14-12. You should save this configuration to the startup configuration so that the switch will boot up in VTP transparent mode. Otherwise, you will lose extended-range VLAN configuration if the switch resets.
- VLANs in the extended range are not supported by VQP. They cannot be configured by VMPS.
- STP is enabled by default on extended-range VLANs, but you can disable it by using the **no spanning-tree vlan** *vlan-id* global configuration command. When the maximum number of spanning-tree instances (64) are on the switch, spanning tree is disabled on any newly created VLANs. If the number of VLANs on the switch exceeds 64, we recommend that you configure the IEEE 802.1S Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 11, "Configuring RSTP and MSTP."

Creating an Extended-Range VLAN

You create an extended-range VLAN in global configuration mode by entering the **vlan** global configuration command with a VLAN ID from 1006 to 4094. This command accesses the config-vlan mode. The extended-range VLAN has the default Ethernet VLAN characteristics (see Table 13-3) and the MTU size is the only parameter you can change. Refer to the description of the **vlan** global configuration command in the *Catalyst 2950 Desktop Switch Command Reference* for defaults of all parameters. If you enter an extended-range VLAN ID when the switch is not in VTP transparent mode, an error message is generated when you exit from config-vlan mode, and the extended-range VLAN is not created.

Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the extended-range VLAN configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to free it up, go to the"Displaying VLANs" section on page 13-16 before creating the extended-range VLAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0881
Doc. 3690

Beginning in privileged EXEC mode, follow these steps to create an extended-range VLAN:

	Command	Purpose
Step 9	**configure terminal**	Enter global configuration mode.
Step 10	**vtp mode transparent**	Configure the switch for VTP transparent mode, disabling VTP.
Step 1	**vlan** *vlan-id*	Enter an extended-range VLAN ID and enter config-vlan mode. The range is 1006 to 4094.
Step 2	**mtu** *mtu-size*	(Optional) Modify the VLAN by changing the MTU size. **Note** Although all commands appear in the CLI help in config-vlan mode, only the **mtu** *mtu-size* command is supported for extended-range VLANs.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vlan id** *vlan-id*	Verify that the VLAN has been created.
Step 5	**copy running-config startup config**	Save your entries in the switch startup configuration file. To save extended-range VLAN configurations, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.

To delete an extended-range VLAN, use the **no vlan** *vlan-id* global configuration command.

The procedure for assigning static-access ports to an extended-range VLAN is the same as for normal-range VLANs. See the "Assigning Static-Access Ports to a VLAN" section on page 13-13.

This example shows how to create a new extended-range VLAN (when the enhanced software image is installed) with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the switch, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. To view normal-range VLANs in the VLAN database (1 to 1005), use the **show** VLAN configuration command (accessed by entering the **vlan database** privileged EXEC command). For a list of the VLAN IDs on the switch, use the **show running-config vlan** privileged EXEC command, optionally entering a VLAN ID range.

Table 13-4 lists the commands for monitoring VLANs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0882
3690
Doc.

Table 13-4 VLAN Monitoring Commands

Command	Command Mode	Purpose
show	VLAN configuration	Display status of VLANs in the VLAN database.
show current [*vlan-id*]	VLAN configuration	Display status of all or the specified VLAN in the VLAN database.
show interfaces [**vlan** *vlan-id*]	Privileged EXEC	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
show running-config vlan	Privileged EXEC	Display all or a range of VLANs on the switch.
show vlan [**id** *vlan-id*]	Privileged EXEC	Display parameters for all VLANs or the specified VLAN on the switch.

For more details about the show command options and explanations of output fields, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

This is an example of output from the **show vlan** privileged EXEC command, showing all VLANs:

```
Switch# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Gi0/1, Gi0/2
2    VLAN0002                         active    Fa0/12
22   VLAN0022                         active    Fa0/7
102  VLAN0102                         active
200  VLAN0200                         active
222  VLAN0222                         active
400  VLAN0400                         active
1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2005 VLAN2005                         active
2006 VLAN2006                         active
2007 VLAN2007                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
22   enet  100022     1500  -      -      -        -    -        0      0
102  enet  100102     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
222  enet  100222     1500  -      -      -        -    -        0      0
400  enet  100400     1500  -      -      -        -    -        0      0
1000 enet  101000     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   -      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
2005 enet  102005     1500  -      -      -        -    -        0      0
2006 enet  102006     1500  -      -      -        -    -        0      0
2007 enet  102007     1500  -      -      -        -    -        0      0
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0883
Doc. 3690

14.982
SA

This is an example of output from the **show vlan brief** privileged EXEC command:

```
Switch# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Gi0/1, Gi0/2
2    VLAN0002                         active    Fa0/12
22   VLAN0022                         active    Fa0/7
102  VLAN0102                         active
200  VLAN0200                         active
222  VLAN0222                         active
400  VLAN0400                         active
1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2005 VLAN2005                         active
2006 VLAN2006                         active
2007 VLAN2007                         active
```

This is an example of output from the **show running-config vlan** command for a range of VLANs:

```
Switch# show running-config vlan 1005-2005
Building configuration...

Current configuration:
!
vlan 1007
!
vlan 1020
!
vlan 1025
!
vlan 2000
!
vlan 2001
end
```

Configuring VLAN Trunks

These sections describe how VLAN trunks function on the switch:

- Trunking Overview, page 13-18
- 802.1Q Configuration Considerations, page 13-20
- Default Layer 2 Ethernet Interface VLAN Configuration, page 13-21

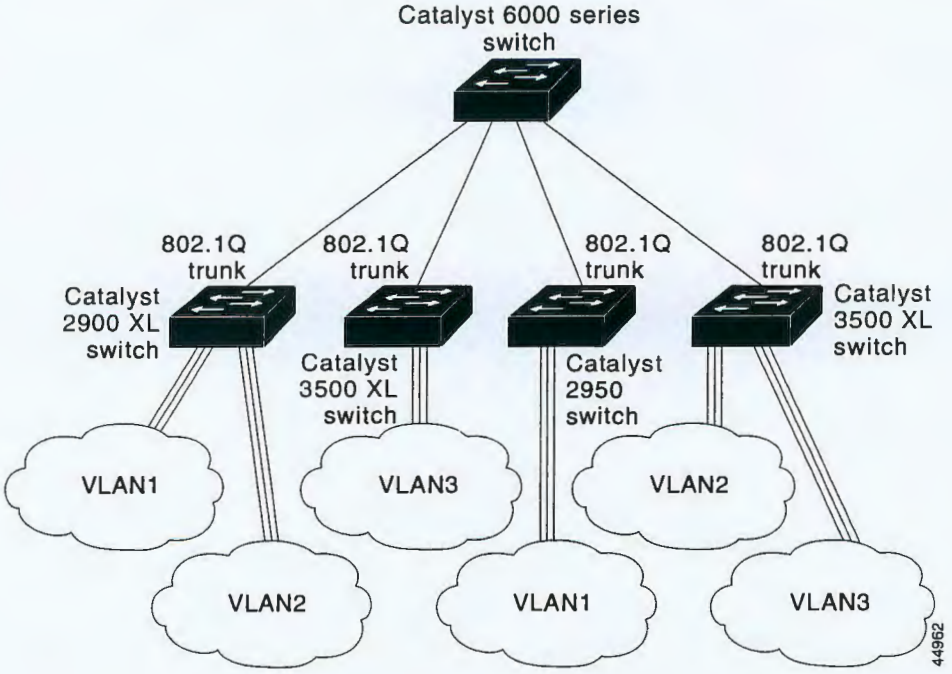
Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Fast Ethernet and Gigabit Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

BOS nº 03/2005 CN
CPMI CORREIOS
Fls. Nº 0884
Doc. 3690

Figure 13-2 shows a network of switches that are connected by 802.1Q trunks.

Figure 13-2 Catalyst 2950, 2900 XL, and 3500 XL Switches in a 802.1Q Trunking Environment



You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see Chapter 25, "Configuring EtherChannels."

Ethernet trunk interfaces support different trunking modes (see Table 13-5). You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0885
Doc. 3690

Table 13-5 Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface is not a trunk interface.
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk*, *desirable*, or *auto* mode. The default switch-port mode for all Ethernet interfaces is **dynamic desirable**.
switchport mode dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk* or *desirable* mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport nonegotiate	Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

802.1Q Configuration Considerations

802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

ECT nº 03/2005 - CN
CPMI - CORREIOS
0390
Fls. Nº
Doc. 3690

14.919
CA

Default Layer 2 Ethernet Interface VLAN Configuration

Table 13-6 shows the default Layer 2 Ethernet interface VLAN configuration.

Table 13-6 Default Layer 2 Ethernet Interface VLAN Configuration

Feature	Default Setting
Interface mode	**switchport mode dynamic desirable**
Allowed VLAN range	VLANs 1–4094 when the enhanced software image is installed and 1 to 1005 when the standard software image is installed
VLAN range eligible for pruning	VLANs 2–1001
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Configuring an Ethernet Interface as a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

This section includes these procedures for configuring an Ethernet interface as a trunk port on the switch:

- Interaction with Other Features, page 13-21
- Defining the Allowed VLANs on a Trunk, page 13-23
- Changing the Pruning-Eligible List, page 13-24
- Configuring the Native VLAN for Untagged Traffic, page 13-25

Note The default mode for Layer 2 interfaces is **switchport mode dynamic desirable**. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk.

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting you entered to all ports in the group:
  - allowed-VLAN list
  - STP port priority for each VLAN
  - STP Port Fast setting
  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.

RQS nº 03/2005 - CN
EPMI - CORREIOS
0887
Fls. Nº
3690
Doc.

- If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as 802.1Q trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface configuration mode and the port to be configured for trunking.
Step 3	**switchport mode {dynamic {auto | desirable} | trunk}**	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode). • **dynamic auto**—Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. • **dynamic desirable**—Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode. • **trunk**—Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 4	**switchport access vlan** *vlan-id*	(Optional) Specify the default VLAN, which is used if the interface stops trunking.
Step 5	**switchport trunk native vlan** *vlan-id*	Specify the native VLAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport**	Display the switchport configuration of the interface in the *Administrative Mode* and the *Administrative Trunking Encapsulation* fields of the display.
Step 8	**show interfaces** *interface-id* **trunk**	Display the trunk configuration of the interface.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration commands to configure the port as a static-access port.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0888
Doc. 3690

This example shows how to configure the Fast Ethernet interface 0/4 as an 802.1Q trunk and shows several ways to verify the configuration. The example assumes that the neighbor interface is configure to support 802.1Q trunking.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/4
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
Switch# show running-config interface fastethernet0/4
Building configuration...

Current configuration : 112 bytes
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 no ip address
 snmp trap link-status
end

Switch# show interfaces fastethernet0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
```

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094 when the enhanced software image is installed, and 1 to 1005 when the standard software image is installed, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **switchport trunk allowed vlan remove** *vlan-list* interface configuration command to remove specific VLANs from the allowed list.

Note You cannot remove VLAN 1 or VLANs 1002 to 1005 from the allowed-VLAN list.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0889
Fls. Nº
Doc. 3690

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the port to be configured.
Step 3	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 4	**switchport trunk allowed vlan** {**add** | **except** | **none** | **remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, **except**, **none**, and **remove** keywords, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default. You cannot remove any of the default VLANs (1 or 1002 to 1005) from a trunk.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking VLANs Enabled* field of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
Switch#
```

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect. The "Enabling VTP Pruning" section on page 14-14 describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and select the trunk port for which VLANs should be pruned.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0890
Fls: Nº
3690
Doc.

	Command	Purpose
Step 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	Configure the list of VLANs allowed to be pruned from the trunk. (See the "VTP Pruning" section on page 14-4). For explanations about using the **add**, **except**, **none**, and **remove** keywords, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Pruning VLANs Enabled* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default pruning-eligible list of all VLANs, use the **no switchport trunk pruning vlan** interface configuration command.

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Note The native VLAN can be assigned any VLAN ID; it is not dependent on the management VLAN.

For information about 802.1Q configuration issues, see the "802.1Q Configuration Considerations" section on page 13-20.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and define the interface that is configured as the 802.1Q trunk.
Step 3	**switchport trunk native vlan** *vlan-id*	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094 when the enhanced software image is installed, and 1 to 1005 when the standard software image is installed. Do not enter leading zeros.
Step 4	**end**	Return to privileged EXEC mode.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0891
Fls. Nº
Doc. 3690

	Command	Purpose
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking Native Mode VLAN* field.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches. For more information about STP, see Chapter 10, "Configuring STP."

Load Sharing Using STP Port Priorities

When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

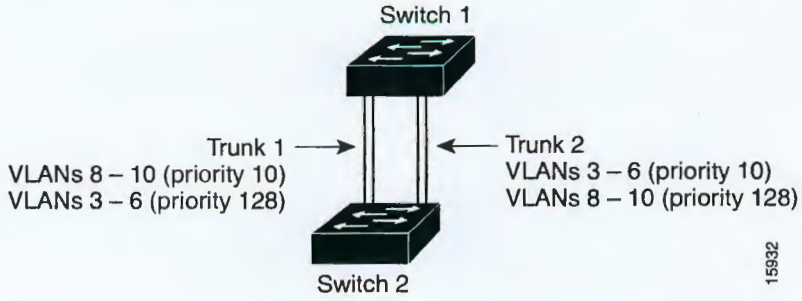
Figure 13-3 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 10 on Trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on Trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2.

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 0892
3690
Doc.

Figure 13-3 Load Sharing by Using STP Port Priorities



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 13-3

	Command	Purpose
Step 1	**vlan database**	On Switch 1, enter VLAN configuration mode.
Step 2	**vtp domain** *domain-name*	Configure a VTP administrative domain. The domain name can be from 1 to 32 characters.
Step 3	**vtp server**	Configure Switch 1 as the VTP server.
Step 4	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 5	**show vtp status**	Verify the VTP configuration on both Switch 1 and Switch 2. In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.
Step 6	**show vlan**	Verify that the VLANs exist in the database on Switch 1.
Step 7	**configure terminal**	Enter global configuration mode.
Step 8	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.
Step 9	**switchport mode trunk**	Configure the port as a trunk port.
Step 10	**end**	Return to privilege EXEC mode.
Step 11	**show interfaces fastethernet0/1 switchport**	Verify the VLAN configuration.
Step 12		Repeat Steps 7 through 11 on Switch 1 for Fast Ethernet port 0/2.
Step 13		Repeat Steps 7 through 11 on Switch 2 to configure the trunk ports on Fast Ethernet ports 0/1 and 0/2.
Step 14	**show vlan**	When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify that Switch 2 has learned the VLAN configuration.
Step 15	**configure terminal**	Enter global configuration mode on Switch 1.
Step 16	**interface fastethernet0/1**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 17	**spanning-tree vlan 8 port-priority 10**	Assign the port priority of 10 for VLAN 8.
Step 18	**spanning-tree vlan 9 port-priority 10**	Assign the port priority of 10 for VLAN 9.
Step 19	**spanning-tree vlan 10 port-priority 10**	Assign the port priority of 10 for VLAN 10.

RQS nº 03/2005 - CN
CPMI CORREIOS
0893
Doc. 3690

	Command	Purpose
Step 20	**exit**	Return to global configuration mode.
Step 21	**interface fastethernet0/2**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 22	**spanning-tree vlan 3 port-priority 10**	Assign the port priority of 10 for VLAN 3.
Step 23	**spanning-tree vlan 4 port-priority 10**	Assign the port priority of 10 for VLAN 4.
Step 24	**spanning-tree vlan 5 port-priority 10**	Assign the port priority of 10 for VLAN 5.
Step 25	**spanning-tree vlan 6 port-priority 10**	Assign the port priority of 10 for VLAN 6.
Step 26	**end**	Return to privileged EXEC mode.
Step 27	**show running-config**	Verify your entries.
Step 28	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

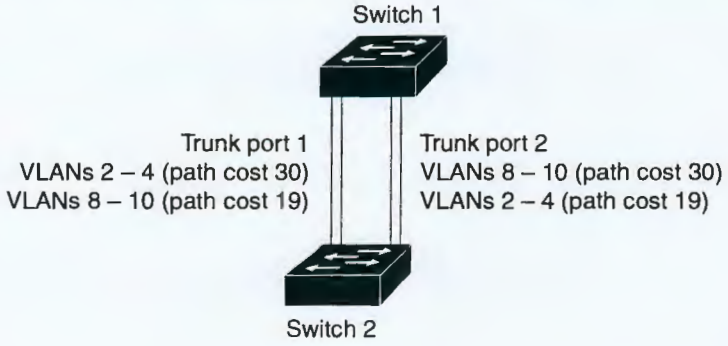
Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs. The VLANs keep the traffic separate. Because no loops exist, STP does not disable the ports, and redundancy is maintained in the event of a lost link.

In Figure 13-4, Trunk ports 1 and 2 are 100BASE-T ports. The path costs for the VLANs are assigned as follows:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1.
- VLANs 8 through 10 retain the default 100BASE-T path cost on Trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2.
- VLANs 2 through 4 retain the default 100BASE-T path cost on Trunk port 2 of 19.

Figure 13-4 Load-Sharing Trunks with Traffic Distributed by Path Cost



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 13-4:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch 1.
Step 2	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0894
Doc. 3690

	Command	Purpose
Step 3	**switchport mode trunk**	Configure the port as a trunk port.
Step 4	**exit**	Return to global configuration mode.
Step 5		Repeat Steps 2 through 4 on Switch 1 interface Fast Ethernet 0/2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries. In the display, make sure that interfaces Fast Ethernet 0/1 and Fast Ethernet 0/2 are configured as trunk ports.
Step 8	**show vlan**	When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration.
Step 9	**configure terminal**	Enter global configuration mode.
Step 10	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to set the STP cost.
Step 11	**spanning-tree vlan 2 cost 30**	Set the spanning-tree path cost to 30 for VLAN 2.
Step 12	**spanning-tree vlan 3 cost 30**	Set the spanning-tree path cost to 30 for VLAN 3.
Step 13	**spanning-tree vlan 4 cost 30**	Set the spanning-tree path cost to 30 for VLAN 4.
Step 14	**end**	Return to global configuration mode.
Step 15		Repeat Steps 9 through 11 on Switch 1 interface Fast Ethernet 0/2, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.
Step 16	**exit**	Return to privileged EXEC mode.
Step 17	**show running-config**	Verify your entries. In the display, verify that the path costs are set correctly for interfaces Fast Ethernet 0/1 and 0/2.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0895
Doc. 3690

Configuring VMPS

The Catalyst 2950 switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through the VLAN Query Protocol (VQP). VMPS dynamically assigns dynamic access port VLAN membership.

This section includes this information about configuring VMPS:

- "Understanding VMPS" section on page 13-30
- "Default VMPS Configuration" section on page 13-33
- "VMPS Configuration Guidelines" section on page 13-33
- "Configuring the VMPS Client" section on page 13-34
- "Monitoring the VMPS" section on page 13-36
- "Troubleshooting Dynamic Port VLAN Membership" section on page 13-37
- "VMPS Configuration Example" section on page 13-37

Understanding VMPS

When the VMPS receives a VQP request from a client switch, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in secure mode. Secure mode determines whether the server shuts down the port when a VLAN is not allowed on it or just denies the port access to the VLAN.

In response to a request, the VMPS takes one of these actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:
  - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.
  - If the VLAN is not allowed on the port and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.
  - If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch receives an *access-denied* response from the VMPS, it continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI, CMS, or SNMP.

You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response, depending on the VMPS secure mode setting.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.-Nº 0896
Doc. 3690

Dynamic Port VLAN Membership

A dynamic (nontrunking) port on the switch can belong to only one VLAN, with a VLAN ID from 1 t 1005. When the link comes up, the switch does not forward traffic to or from this port until the VMP provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of new host connected to the dynamic port and attempts to match the MAC address to a VLAN in the VMP database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the quer packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packe matches its own domain name before accepting the request and responds to the client with the assigne VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down th port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN; however, the VMPS shuts down a dynamic port if more than 20 hosts are active on the port.

If the link goes down on a dynamic port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMP before the port is assigned to a VLAN.

VMPS Database Configuration File

The VMPS contains a database configuration file that you create. This ASCII text file is stored on a switch-accessible TFTP server that functions as a VMPS server. The file contains VMPS information, such as the domain name, the fallback VLAN name, and the MAC-address-to-VLAN mapping. The Catalyst 2950 switch cannot act as the VMPS, but you can use a Catalyst 5000 or Catalyst 6000 series switch as the VMPS.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

Whenever port names are used in the VMPS database configuration file, the server must use the switch convention for naming ports. For example, Fa0/4 is fixed Fast Ethernet port number 4. If the switch is a cluster member, the command switch adds the name of the switch before the type. For example, *es3%Fa0/4* refers to fixed Fast Ethernet port 4 on member switch 3. When port names are required, these naming conventions must be followed in the VMPS database configuration file when it is configured to support a cluster.

This example shows a example of a VMPS database configuration file as it appears on a Catalyst 6000 series switch. The file has these characteristics:

- The security mode is open.
- The default is used for the fallback VLAN.
- MAC address-to-VLAN name mappings—The MAC address of each host and the VLAN to which each host belongs is defined.
- Port groups are defined.
- VLAN groups are defined.
- VLAN port policies are defined for the ports associated with restricted VLANs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0897
Doc. 3690

```
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain DSBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
 device 198.92.30.32 port 0/2
 device 172.20.26.141 port 0/8
vmps-port-group "Executive Row"
 device 198.4.254.222 port 0/2
 device 198.4.254.222 port 0/3
 device 198.4.254.223 all-ports
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name>
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
 port-group WiringCloset1
vmps-port-policies vlan-name Green
 device 198.92.30.32 port 0/8
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0898
Doc. 3690

```
vmps-port-policies vlan-name Purple
 device 198.4.254.22 port 0/2
 port-group "Executive Row"
```

Default VMPS Configuration

Table 13-7 shows the default VMPS and dynamic port configuration on client switches.

Table 13-7 Default VMPS Client and Dynamic Port Configuration

Feature	Default Setting
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic ports	None configured

VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic port VLAN membership:

- You must configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. For the cluster-based port-naming conventions, see the "VMPS Database Configuration File" section on page 13-31.
- When you configure a port as dynamic, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state. You can disable Port Fast mode on a dynamic port.
- 802.1X ports cannot be configured as dynamic ports. If you try to enable 802.1X on a dynamic-access (VQP) port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic access setting takes effect.
- Dynamic ports cannot be network ports or monitor ports.
- Secure ports cannot be dynamic ports. You must disable port security on a port before it becomes dynamic.
- Dynamic ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic ports.
- The VTP management domain of the VMPS client and the VMPS server must be the same.
- VQP does not support extended-range VLANs (VLAN IDs higher than 1006). Extended-range VLANs cannot be configured by VMPS.
- The VLAN configured on the VMPS server should not be a voice VLAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0899
3690
Doc.

Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch can be a VMPS client; it cannot be a VMPS server.

Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch as a client.

Note If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps server** *ipaddress* **primary**	Enter the IP address of the switch acting as the primary VMPS server.
Step 3	**vmps server** *ipaddress*	Enter the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vmps**	Verify your entries in the *VMPS Domain Server* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The switch port that is connected to the VMPS server cannot be a dynamic access port. It can be either a static access port or a trunk port. See the "Configuring an Ethernet Interface as a Trunk Port" section on page 13-21.

Configuring Dynamic Access Ports on VMPS Clients

If you are configuring a port on a cluster member switch as a dynamic port, first use the **rcommand** privileged EXEC command to log into the member switch.

Caution Dynamic port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic access ports to other switches can cause a loss of connectivity.

Beginning in privileged EXEC mode, follow these steps to configure a dynamic access port on a VMPS client switch:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the switch port that is connected to the end station.
Step 3	**switchport mode access**	Set the port to access mode.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 900
3690
Doc.

	Command	Purpose
Step 4	**switchport access vlan dynamic**	Configure the port as eligible for dynamic VLAN membership. The dynamic access port must be connected to an end station.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Operational Mode* field of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To return an interface to its default switchport mode (dynamic desirable), u the **no switchport mode** interface configuration command. To reset the access mode to the default VLAN for the switch, use the **no switchport access** interface configuration command.

Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic port VLAN membersh assignments that the switch has received from the VMPS:

	Command	Purpose
Step 1	**vmps reconfirm**	Reconfirm dynamic port VLAN membership.
Step 2	**show vmps**	Verify the dynamic VLAN reconfirmation status.

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. Y can set the number of minutes after which reconfirmation occurs.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than t reconfirmation setting on the command switch. You must also first use the **rcommand** privileged EXE command to log into the member switch.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps reconfirm** *minutes*	Enter the number of minutes between reconfirmations of the dynamic VLAN membership. Enter a number from 1 to 120. The default is 60 minutes.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps reconfirm** global configuration command

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0901
3690
Doc.

14.964

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps retry** *count*	Change the retry count. The retry range is from 1 to 10; the default is 3.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify your entry in the *Server Retry Count* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps retry** global configuration command.

Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The switch displays this information about the VMPS:

VMPS VQP Version — The version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP version 1.

Reconfirm Interval — The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.

Server Retry Count — The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.

VMPS domain server — The IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked *current*. The one marked *primary* is the primary server.

VMPS Action — The result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expired, or you can force it by entering the **vmps reconfirm** privileged EXEC command or its CMS or SNMP equivalent.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0902
Doc. 3690

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps

VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:          No Dynamic Port
```

Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shut down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic port.

To re-enable a disabled dynamic port, enter the **no shutdown** interface configuration command.

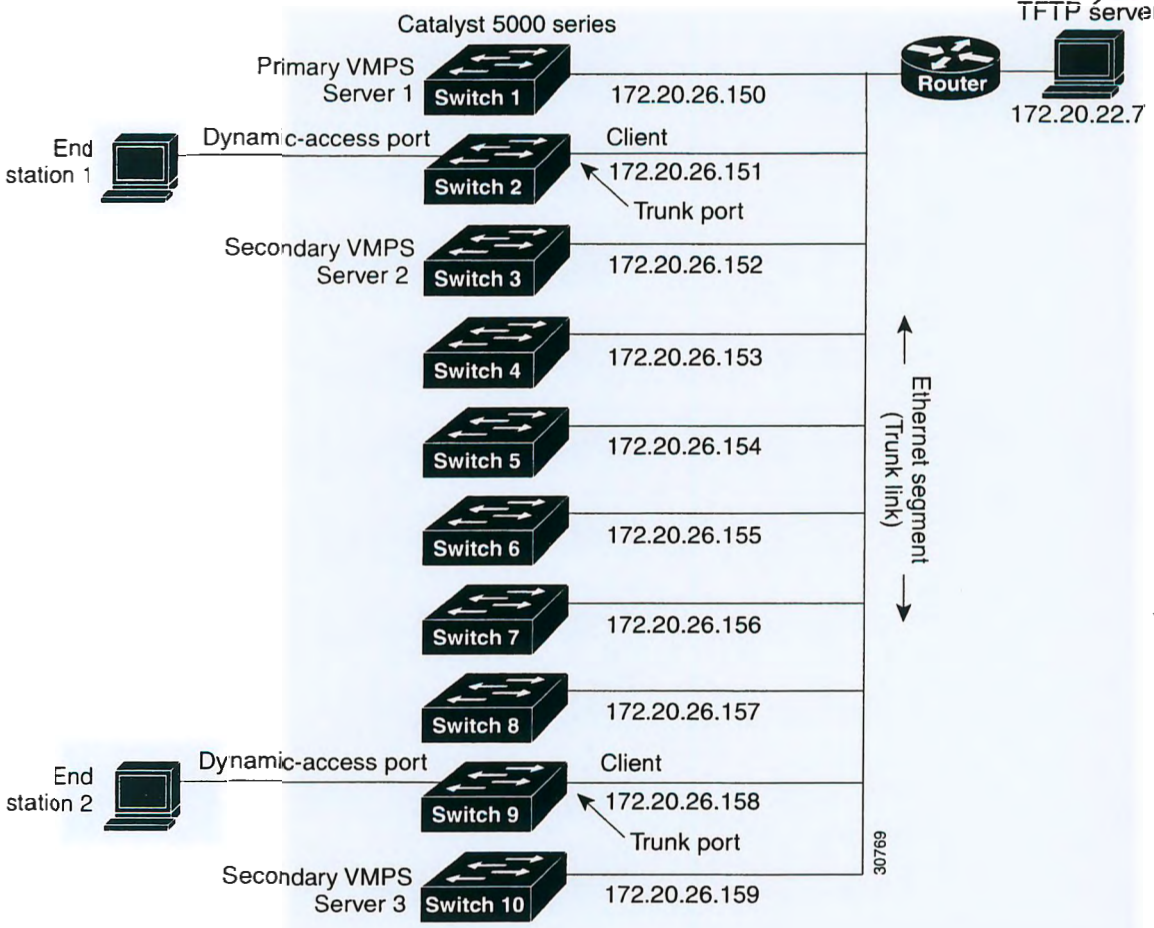
VMPS Configuration Example

Figure 13-5 shows a network with a VMPS server switch and VMPS client switches with dynamic ports In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 5000 series Switch 1 is the primary VMPS server.
- The Catalyst 5000 series Switch 3 and Switch 10 are secondary VMPS servers.
- The end stations are connected to these clients:
  - Catalyst 2950 Switch 2
  - Catalyst 3500 XL Switch 9
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0903
Doc. 3690

Figure 13-5 Dynamic Port VLAN Membership Configuration



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0904
Doc. 3690

14-87
A

Switch Tipo 2 doc 5

RQS nº 03/2005 - CN
CPMI - - - CORREIOS
Fls. Nº 0905
Doc. 3690

14.874
A.

CiscoWorks CiscoView 5.4

THE CISCOVIEW DEVICE MANAGER IS THE MOST WIDELY DEPLOYED DEVICE MANAGEMENT SOFTWAR APPLICATION PROVIDED BY CISCO. BEING WEB-BASED, CISCOWORKS CISCOVIEW ALLOWS UBIQUITOU ACCESS FROM ANY CLIENT WITH A STANDARD BROWSER, NETWORK ACCESS, AND MINIMUM HARDWAR REQUIREMENTS. USERS CONTINUE TO RELY ON THE INTUITIVE INTERFACE, REAL-TIME DEVICE MONITORIN AND EASY DEVICE CONFIGURATION IN CISCOVIEW, AS WELL AS NEW FEATURES THAT ENHANCE I FUNCTIONALITY. EASILY INTEGRATED WITH CISCOWORKS PRODUCTS OR PARTNER PLATFORMS, CISCOVIE PROVIDES MULTI-USER DEVICE MANAGEMENT IN THE LARGER CONTEXT OF AN END-TO-END MANAGEMEN INTRANET SOLUTION.

CiscoView Web-based management aides network management by displaying a physical view of Cisco devices and color-coding device ports for at-a-glance port status, allowing users to quickly grasp essential information. CiscoView features provide dynamic status, device monitoring, and comprehensive configuration information for Cisco internetworking products (routers, switches, and access products). Features include:

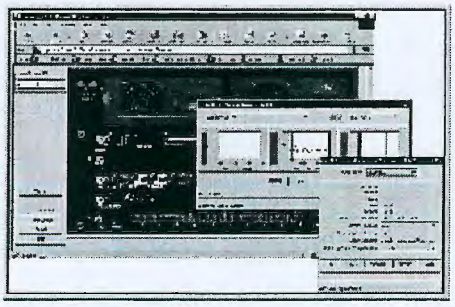
- Web-based displays of Cisco products from a single location, giving network managers a complete view of Cisco products without physically checking each device (see Figure 1)
- A continuously updated physical view of routers, hubs, switches, or access servers in a network
- Real-time monitoring and tracking of key information and data relating to device performance, traffic, and environment, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators
- The ability to modify device configurations across router, switch, and access server products.
- The ability to access the support for existing and new Cisco devices via the Web-based Package Support Updater (PSU), without having to purchase and install new versions of CiscoView
- Multi-user access to a single CiscoView server through a Web-based client

New CiscoView 5.4 Features

CiscoView 5.4 has several new features including:

- New device support
- Secure communication between the client browser and the server via Secure Sockets Layer (SSL) protocol
- Device list import from local RME through SSL

Figure 1 CiscoView 5



Common Management Foundation

CiscoView 5.4 uses many of the components in the CiscoWork common management foundation. An integration utility is available to all CiscoWorks applications to provide integration with third-party network management systems (NMSs). This utility adds CiscoView device-specific information to the NMS and provides launch points to other Cisco applications, creating seamless management environment for the end user. The utility modular, independent design allows:

- Integration between applications residing on different servers and even different operating systems
- Dynamic updates to integration information in the NMS
- Dynamic upgrades to new versions of the NMS, without reinstalling CiscoWorks
- Flexibility in customizing your management intranet environment using totally Web-based tools from Cisco

NMS support is updated frequently, and files can be downloade from CCO by referring to the CiscoView planner page: http:// www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi

ROS nº 03/2005 - CN
CPMI - CORREIOS
0006
3690
Doc.

CISCO SYSTEMS

14.813
A.

More Information

For more information on CiscoView see the CiscoView Upgrade Planner at http://www.cisco.com/public/sw-center/sw-netmgmt.shtml Server, Client, and Web Browser Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions, and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Device Support

The modular design of CiscoView allows users to add support for devices as necessary. Device support files can be downloaded through the Web-based CiscoView Package Support Updater (PSU), located on the CiscoWorks desktop. The PSU is used for scheduled and on-demand device support downloads from CCO. To find more information on downloading device packages, please click on this URL:. http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cvparnt/cview/cv4gsg/cvgsdld.htm#xtocid238445

To get the most recent list of devices supported, see: http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi

Ordering Information

CiscoView is sold as an integral part of several Cisco solutions, and is not sold as an individual product.

The Routed WAN Management Solution and the LAN Management Solution contain CiscoView, as does CiscoWorks for Windows.

Availability

CiscoView is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For more information on CiscoView and on the CiscoWorks family of products, see: http://cisco.com/warp/public/cc/pd/wr2k/

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0907
3690
Doc.

14-872
A.

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

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: 61 2 8448 7100
Fax: 61 2 9957 4350

RQS nº 03/2005 - CN
CPMI - CORREIOS
0908
Fls. Nº
Doc. 3090

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000, Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0007R)

09/00 BW6624

Switch Tipo 2 doc 6

RQS nº 03/2005 - CN
CPMI CORREIOS
0909
Fls. Nº
Doc. 3690

Hierarchical Navigation
Skip to Content
TECHNOLOGIES
LAN SWITCHING
PROTOCOL GROUPS
ETHERNET
PROTOCOLS
Carrier Sense Multiple Access (CSMA)
Ethernet (802.3)
Fast Ethernet (802.3u)
Gigabit Ethernet (802.3z)
Gigabit Ethernet over copper (802.3ab)
Long-Reach Ethernet
Speed / Duplex negotiation
UniDirectional Link Detection (UDLD)
10 Gigabit Ethernet

- Gigabit Ethernet over copper (802.3ab)

Introduction

Gigabit ethernet over Copper (also known as 1000BaseT) is an extension of the existing Fast Ethernet standard. It specifies Gigabit Ethernet operation over the Category 5e/6 cabling systems already installed, making it a highly cost effective solution. As a result, most copper-based environments that run Fast Ethernet can also run Gigabit Ethernet over the existing network infrastructure in order to dramatically boost network performance for demanding applications.

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0910
Fls. Nº
3690
Doc.

14.914
A

Switch Tipo 2 doc 4

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0911
3690
Doc.

14.913
A-

CHAPTER 13

Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094). It includes information about VLAN modes and the VLAN Membership Policy Server (VMPS).

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

The chapter includes these sections:

- Understanding VLANs, page 13-1
- Configuring Normal-Range VLANs, page 13-6
- Configuring Extended-Range VLANs, page 13-14
- Displaying VLANs, page 13-16
- Configuring VLAN Trunks, page 13-18
- Configuring VMPS, page 13-30

Understanding VLANs

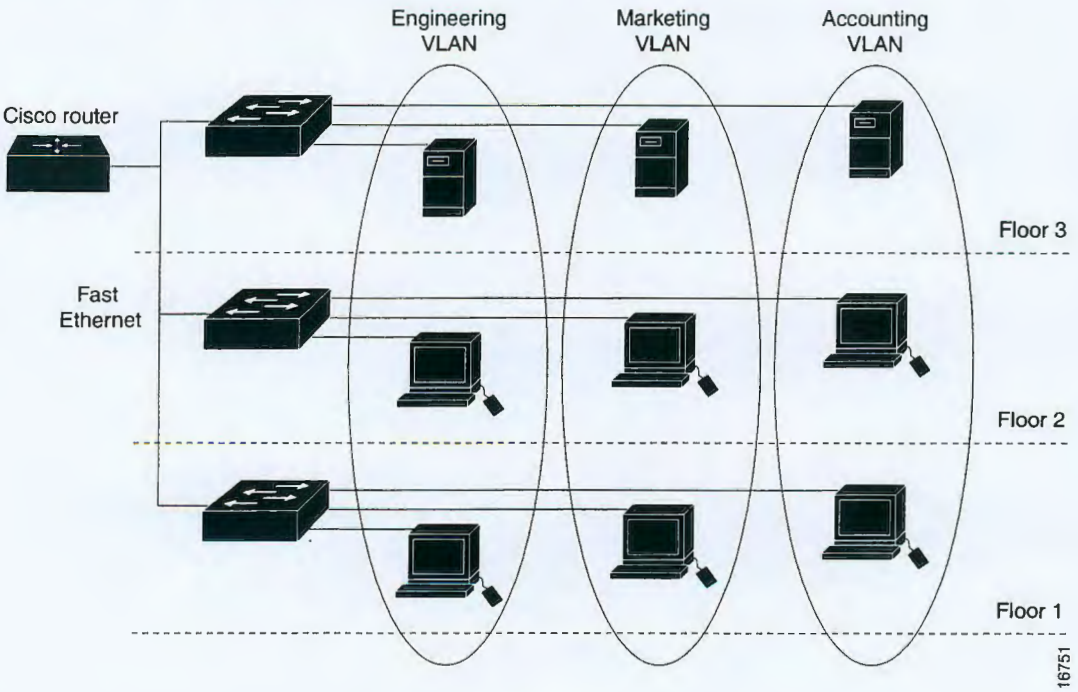
A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge as shown in Figure 13-1. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree. See Chapter 10, "Configuring STP" and Chapter 11, "Configuring RSTP and MSTP."

Note Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network. For more information on VTP, see Chapter 14, "Configuring VTP."

ECT nº 03/2005 - GN
CPMI - CORREIOS
Fls. 0012
Doc. 3690

Figure 13-1 shows an example of VLANs segmented into logically defined networks.

Figure 13-1 VLANs as Logically Defined Networks



VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Supported VLANs

Table 13-1 lists the number of supported VLANs on Catalyst 2950 switches.

Table 13-1 Maximum Number of Supported VLANs

Switch Model	Number of Supported VLANs
Catalyst 2950-12	64
Catalyst 2950-24	64
Catalyst 2950C-24	250
Catalyst 2950G-12-EI	250
Catalyst 2950G-24-EI	250
Catalyst 2950G-48-EI	250
Catalyst 2950G-24-EI-DC	250
Catalyst 2950T-24	250

RQS nº 03/2005 - CN
CPMI - CORREIOS
0913
Fls. Nº
Doc. 3690

VLANs are identified with a number from 1 to 4094 when the enhanced software image is installed and 1 to 1005 when the standard software image is installed. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VTP only learns normal-range VLANs, with VLAN IDs 1 to 1005; VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database. The switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094.

The switch supports per-VLAN spanning tree (PVST) with a maximum of 64 spanning-tree instances. One spanning-tree instance is allowed per VLAN. See the "Configuration Guidelines for Normal-Range VLANs" section on page 13-7 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

Note The Catalyst 2950 switches do not support Inter-Switch Link (ISL) trunking.

Management VLANs

Communication with the switch management interfaces is through the switch IP address. The IP address is associated with the management VLAN, which by default is VLAN 1.

The management VLAN has these characteristics:

- It is created from CMS or through the CLI on static-access, dynamic-access, and trunk ports. You cannot create or remove the management VLAN through Simple Network Management Protocol (SNMP).
- Only one management VLAN can be administratively active at a time.
- With the exception of VLAN 1, the management VLAN can be deleted.
- When created, the management VLAN is administratively down.

Before changing the management VLAN on your switch network, make sure you follow these guidelines:

- The new management VLAN should not have a Hot Standby Router Protocol (HSRP) standby group configured on it.
- You must be able to move your network management station to a switch port assigned to the same VLAN as the new management VLAN.
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.
- On switches running a IOS software version that is earlier than Cisco IOS 12.0(5)XP, you cannot change the management VLAN. Switches running Cisco IOS 12.0(5)XP should be upgraded to the current software release as described in the release notes.

If you are using SNMP or CMS to manage the switch, ensure that the port through which you are connected to a switch is in the management VLAN.

For information about the role management VLANs play in switch clusters, see the "Management VLAN" section on page 6-20.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0914
Fls. Nº
3690
Doc.

14.910
JA.

Determining the Management VLAN for a New Switch

If you add a new switch to an existing cluster and the cluster is using a management VLAN other than the default VLAN 1, the command switch automatically senses that the new switch has a different management VLAN and has not been configured. The command switch issues commands to change the management VLAN on the new switch to match the one used by the cluster. This automatic change occurs for new, out-of-box switches that do not have a config.text file and for which there have been no changes to the running configuration.

Before a new switch can be added to a cluster, it must be connected to a port that belongs to the cluster management VLAN. If the cluster is configured with a management VLAN other than the default, the command switch changes the management VLAN for new switches when they are connected to the cluster. In this way, the new switch can exchange Cisco Discovery Protocol (CDP) messages with the command switch and be proposed as a cluster candidate.

Note For the command switch to change the management VLAN on a new switch, there must have been no changes to the new switch configuration, and there must be no config.text file.

Because the switch is new and unconfigured, its management VLAN is changed to the cluster management VLAN when it is first added to the cluster. All ports that have an active link at the time of this change become members of the new management VLAN.

For information about the role management VLANs play in switch clusters, see the "Management VLAN" section on page 6-20.

Changing the Management VLAN for a Cluster

Beginning in privileged EXEC mode on the command switch, follow these steps to configure the management VLAN interface through a Telnet or Secure Shell (SSH) connection:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cluster management-vlan** *vlanid*	Change the management VLAN for the cluster. This ends your Telnet session. Change the port through which you are connected to the switch to a port in the new management VLAN.
Step 3	**show running-config**	Verify the change.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0915
Doc. 3690

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that determines the kind of traffic the port carries and the number of VLANs to which it can belong. Table 13-2 lists the membership modes and membership and VTP characteristics.

Table 13-2 Port Membership Modes

Membership Mode	VLAN Membership Characteristics	VTP Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 13-13.	VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent to disable VTP. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.
802.1Q trunk	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list. For information about configuring trunk ports, see the "Configuring an Ethernet Interface as a Trunk Port" section on page 13-21.	VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.
Dynamic access	A dynamic-access port can belong to one normal-range VLAN (VLAN ID 1 to 1005) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6000 series switch, for example, but never a Catalyst 2950 switch. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station and not to another switch. For configuration information, see the "Configuring Dynamic Access Ports on VMPS Clients" section on page 13-34.	VTP is required. Configure the VMPS and the client with the same VTP domain name. You can change the reconfirmation interval and retry count on the VMPS client switch.

For more detailed definitions of the modes and their functions, see Table 13-5 on page 13-20.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the "Managing the MAC Address Table" section on page 7-52.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0916
Doc. 3690

Configuring Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. If the switch is in VTP server or transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

Note When the switch is in VTP transparent mode and the enhanced software image is installed, you can also create extended-range VLANs (VLANs with IDs from 1006 to 4094), but these VLANs are not saved in the VLAN database. See the "Configuring Extended-Range VLANs" section on page 13-14.

Configurations for VLAN IDs 1 to 1005 are written to the file *vlan.dat* (VLAN database), and you can display them by entering the **show vlan** privileged EXEC command. The *vlan.dat* file is stored in nonvolatile RAM (NVRAM).

Caution You can cause inconsistency in the VLAN database if you attempt to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the *Catalyst 2950 Desktop Switch Command Reference* for this release. To change the VTP configuration, see Chapter 14, "Configuring VTP."

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

Note This section does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0917
Doc. 3690

14.907
A-

This section includes information about these topics about normal-range VLANs:

- Token Ring VLANs, page 13-7
- Configuration Guidelines for Normal-Range VLANs, page 13-7
- VLAN Configuration Mode Options, page 13-8
- Saving VLAN Configuration, page 13-9
- Default Ethernet VLAN Configuration, page 13-10
- Creating or Modifying an Ethernet VLAN, page 13-10
- Deleting a VLAN, page 13-12
- Assigning Static-Access Ports to a VLAN, page 13-13

Token Ring VLANs

Although the Catalyst 2950 switches do not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running VTP version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, refer to the *Catalyst 5000 Series Software Configuration Guide*.

Configuration Guidelines for Normal-Range VLANs

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- See Table 13-1 for the maximum number of supported VLANs per switch model. On a switch supporting 250 VLANs, if VTP reports that there are 254 active VLANs, four of the active VLANs (1002 to 1005) are reserved for Token Ring and FDDI.
- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- VLAN configuration for VLANs 1 to 1005 are always saved in the VLAN database. If VTP mode is transparent, VTP and VLAN configuration is also saved in the switch running configuration file.
- The switch also supports VLAN IDs 1006 through 4094 in VTP transparent mode (VTP disabled) when the enhanced software image is installed. These are extended-range VLANs and configuration options are limited. Extended-range VLANs are not saved in the VLAN database. See the "Configuring Extended-Range VLANs" section on page 13-14.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.
- Catalyst 2950 switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.
- The switch supports 64 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 64 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls Nº 0918
Doc. 3690

14. 906

running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch exceeds 64, we recommend that you configure the IEEE 802.1S Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 11, "Configuring RSTP and MSTP."

VLAN Configuration Mode Options

You can configure normal-range VLANs (with VLAN IDs 1 to 1005) by using these two configuration modes:

- VLAN Configuration in config-vlan Mode, page 13-8

  You access config-vlan mode by entering the **vlan** *vlan-id* global configuration command.

- VLAN Configuration in VLAN Configuration Mode, page 13-8

  You access VLAN configuration mode by entering the **vlan database** privileged EXEC command.

VLAN Configuration in config-vlan Mode

To access config-vlan mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN or with an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 13-3) or enter multiple commands to configure the VLAN. For more information about commands available in this mode, refer to the **vlan** global configuration command description in the *Catalyst 2950 Desktop Switch Command Reference* for this release. When you have finished the configuration, you must exit config-vlan mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

You must use this config-vlan mode when creating extended-range VLANs (VLAN IDs greater than 1005). See the "Configuring Extended-Range VLANs" section on page 13-14.

VLAN Configuration in VLAN Configuration Mode

To access VLAN configuration mode, enter the **vlan database** privileged EXEC command. Then enter the **vlan** command with a new VLAN ID to create a VLAN or with an existing VLAN ID to modify the VLAN. You can use the default VLAN configuration (Table 13-3) or enter multiple commands to configure the VLAN. For more information about keywords available in this mode, refer to the **vlan** VLAN configuration command description in the *Catalyst 2950 Desktop Switch Command Reference* for this release. When you have finished the configuration, you must enter **apply** or **exit** for the configuration to take effect. When you enter the **exit** command, it applies all commands and updates the VLAN database. VTP messages are sent to other switches in the VTP domain, and the privileged EXEC mode prompt appears.

RQS-nº 03/2005 - CN
CPMI CORREIOS
0919
Fls. Nº
Doc. 3690

14-905
A

Saving VLAN Configuration

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file). If VTP mode is transparent, they are also saved in the switch running configuration file and you can enter the **copy running-config startup-config** privileged EXEC command to save the configuration in the startup configuration file. You can use the **show running-config vlan** privileged EXEC command to display the switch running configuration file. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is determined as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the first 1005 VLANs use the VLAN database information.
- If VTP mode is server, the domain name and VLAN configuration for the first 1005 VLANs use the VLAN database information
- If the switch is running IOS release 12.1(9)EA1 or later and you use an older startup configuration file to boot up the switch, the configuration file does not contain VTP or VLAN information, and the switch uses the VLAN database configurations.
- If the switch is running an IOS release earlier than 12.1(9)EA1 and you use a startup configuration file from IOS release 12.1(9)EA1 or later to boot up the switch, the image on the switch does not recognize the VLAN and VTP configurations in the startup configuration file, so the switch uses the VLAN database configuration.

Caution If the startup configuration file contains extended-range VLAN configuration, this information will be lost when the system boots up.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0920
Doc. 3690

Default Ethernet VLAN Configuration

Table 13-3 shows the default configuration for Ethernet VLANs.

Note The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

Table 13-3 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094 when the enhanced software image is installed and 1 to 1005 when the standard software image is installed. **Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	*VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number	No range
802.10 SAID	100001 (100000 plus the VLAN ID)	1–4294967294
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Creating or Modifying an Ethernet VLAN

Each Ethernet VLAN in the VLAN database has a unique, 4-digit ID that can be a number from 1 to 1001. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs. To create a normal-range VLAN to be added to the VLAN database, assign a number and name to the VLAN.

Note When the switch is in VTP transparent mode and the enhanced software image is installed, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database. See the "Configuring Extended-Range VLANs" section on page 13-14.

For the list of default parameters that are assigned when you add a VLAN, see the "Configuring Normal-Range VLANs" section on page 13-6.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0921
Doc. 3690

Beginning in privileged EXEC mode, follow these steps to use config-vlan mode to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID, and enter config-vlan mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify a VLAN. **Note** The available VLAN ID range for this command is 1 to 1005 when the standard software image is installed and 1 to 4094 when the enhanced software image is installed; do not enter leading zeros. For information about adding VLAN IDs greater than 1005 (extended-range VLANs), see the "Configuring Extended-Range VLANs" section on page 13-14.
Step 3	**name** *vlan-name*	(Optional) Enter a name for the VLAN. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 4	**mtu** *mtu-size*	(Optional) Change the MTU size (or other VLAN characteristic).
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries.
Step 7	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To return the VLAN name to the default settings, use the **no vlan name** or **no vlan mtu** config-vlan commands.

This example shows how to use config-vlan mode to create Ethernet VLAN 20, name it *test20,* and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

Beginning in privileged EXEC mode, follow these steps to use VLAN configuration mode to create or modify an Ethernet VLAN:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**vlan** *vlan-id* **name** *vlan-name*	Add an Ethernet VLAN by assigning a number to it. The range is 1 to 1001; do not enter leading zeros. If no name is entered for the VLAN, the default is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.
Step 3	**vlan** *vlan-id* **mtu** *mtu-size*	(Optional) To modify a VLAN, identify the VLAN and change a characteristic, such as the MTU size

RQS nº 03/2005 - CN
CPMI 0632 CORREIOS
Fls. Nº
3690
Doc.

	Command	Purpose
Step 4	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 5	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}	Verify your entries.
Step 6	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To return the VLAN name to the default settings, use the **no vlan** *vlan-id* **name** or **no vlan** *vlan-id* **mtu** VLAN configuration command.

This example shows how to use VLAN configuration mode to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# vlan database
Switch(vlan)# vlan 20 name test20
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

Deleting a VLAN

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch by using global configuration mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no vlan** *vlan-id*	Remove the VLAN by entering the VLAN ID.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vlan brief**	Verify the VLAN removal.
Step 5	**copy running-config startup config**	(Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup configuration file.

To delete a VLAN by using VLAN configuration mode, use the **vlan database** privileged EXEC command to enter VLAN configuration mode and the **no vlan** *vlan-id* VLAN configuration command.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0053
Fls. Nº
3690
Doc.

14-901
A-

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information (VTP is disabled). If you are assigning a port on a cluster member switch to a VLAN, first use the **rcommand** privileged EXEC command to log in to the member switch.

Note If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 13-10.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode
Step 2	**interface** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).
Step 4	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094; do not enter leading zeros.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config interface** *interface-id*	Verify the VLAN membership mode of the interface.
Step 7	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

This example shows how to configure Fast Ethernet interface 0/1 as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
Switch#
```

These examples show how to verify the configuration:

```
Switch# show running-config interface fastethernet0/1
Building configuration...

Current configuration : 74 bytes
!
interface FastEthernet0/12
 switchport access vlan 2
 switchport mode access
end
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0924
3690
Doc.

```
Switch# show interfaces fastethernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (VLAN0002)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Voice VLAN: none (Inactive)
Appliance trust: none
```

Configuring Extended-Range VLANs

When the switch is in VTP transparent mode (VTP disabled) and the enhanced software image is installed), you can create extended-range VLANs (in the range 1006 to 4094). Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any switchport commands that allow VLAN IDs. You always use config-vlan mode (accessed by entering the **vlan** *vlan-id* global configuration command) to configure extended-range VLANs. The extended range is not supported in VLAN configuration mode (accessed by entering the **vlan database** privileged EXEC command).

Extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Although the switch supports 4094 VLAN IDs when the enhanced software image is installed, see the "Supported VLANs" section on page 13-2 for the actual number of VLANs supported.

This section includes this information about extended-range VLANs:

- Default VLAN Configuration, page 13-14
- Configuration Guidelines for Extended-Range VLANs, page 13-15
- Creating an Extended-Range VLAN, page 13-15
- Displaying VLANs, page 13-16

Default VLAN Configuration

See Table 13-3 on page 13-10 for the default configuration for Ethernet VLANs. You can change only the MTU size on extended-range VLANs; all other characteristics must remain at the default state.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0925
Doc. 3690

Configuration Guidelines for Extended-Range VLANs

14.899
A.

Follow these guidelines when creating extended-range VLANs:

- To add an extended-range VLAN, you must use the **vlan** *vlan-id* global configuration command and access config-vlan mode. You cannot add extended-range VLANs in VLAN configuration mode (accessed by entering the **vlan database** privileged EXEC command).
- VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP.
- You cannot include extended-range VLANs in the pruning eligible range.
- The switch must be in VTP transparent mode when you create extended-range VLANs. If VTP mode is server or client, an error message is generated, and the extended-range VLAN is rejected.
- You can set the VTP mode to transparent in global configuration mode or in VLAN configuration mode. See the "Disabling VTP (VTP Transparent Mode)" section on page 14-12. You should save this configuration to the startup configuration so that the switch will boot up in VTP transparent mode. Otherwise, you will lose extended-range VLAN configuration if the switch resets.
- VLANs in the extended range are not supported by VQP. They cannot be configured by VMPS.
- STP is enabled by default on extended-range VLANs, but you can disable it by using the **no spanning-tree vlan** *vlan-id* global configuration command. When the maximum number of spanning-tree instances (64) are on the switch, spanning tree is disabled on any newly created VLANs. If the number of VLANs on the switch exceeds 64, we recommend that you configure the IEEE 802.1S Multiple STP (MSTP) on your switch to map multiple VLANs to a single STP instance. For more information about MSTP, see Chapter 11, "Configuring RSTP and MSTP."

Creating an Extended-Range VLAN

You create an extended-range VLAN in global configuration mode by entering the **vlan** global configuration command with a VLAN ID from 1006 to 4094. This command accesses the config-vlan mode. The extended-range VLAN has the default Ethernet VLAN characteristics (see Table 13-3) and the MTU size is the only parameter you can change. Refer to the description of the **vlan** global configuration command in the *Catalyst 2950 Desktop Switch Command Reference* for defaults of all parameters. If you enter an extended-range VLAN ID when the switch is not in VTP transparent mode, an error message is generated when you exit from config-vlan mode, and the extended-range VLAN is not created.

Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the extended-range VLAN configuration in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to free it up, go to the"Displaying VLANs" section on page 13-16 before creating the extended-range VLAN.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0926
3690
Doc

Beginning in privileged EXEC mode, follow these steps to create an extended-range VLAN:

	Command	Purpose
Step 9	**configure terminal**	Enter global configuration mode.
Step 10	**vtp mode transparent**	Configure the switch for VTP transparent mode, disabling VTP.
Step 1	**vlan** *vlan-id*	Enter an extended-range VLAN ID and enter config-vlan mode. The range is 1006 to 4094.
Step 2	**mtu** *mtu-size*	(Optional) Modify the VLAN by changing the MTU size. **Note** Although all commands appear in the CLI help in config-vlan mode, only the **mtu** *mtu-size* command is supported for extended-range VLANs.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vlan id** *vlan-id*	Verify that the VLAN has been created.
Step 5	**copy running-config startup config**	Save your entries in the switch startup configuration file. To save extended-range VLAN configurations, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.

To delete an extended-range VLAN, use the **no vlan** *vlan-id* global configuration command.

The procedure for assigning static-access ports to an extended-range VLAN is the same as for normal-range VLANs. See the "Assigning Static-Access Ports to a VLAN" section on page 13-13.

This example shows how to create a new extended-range VLAN (when the enhanced software image is installed) with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch startup configuration file:

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the switch, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. To view normal-range VLANs in the VLAN database (1 to 1005), use the **show** VLAN configuration command (accessed by entering the **vlan database** privileged EXEC command). For a list of the VLAN IDs on the switch, use the **show running-config vlan** privileged EXEC command, optionally entering a VLAN ID range.

Table 13-4 lists the commands for monitoring VLANs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0927
Fls. Nº
3690
Doc.

Table 13-4 VLAN Monitoring Commands

Command	Command Mode	Purpose
show	VLAN configuration	Display status of VLANs in the VLAN database.
show current [*vlan-id*]	VLAN configuration	Display status of all or the specified VLAN in the VLAN database.
show interfaces [**vlan** *vlan-id*]	Privileged EXEC	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
show running-config vlan	Privileged EXEC	Display all or a range of VLANs on the switch.
show vlan [**id** *vlan-id*]	Privileged EXEC	Display parameters for all VLANs or the specified VLAN on the switch.

For more details about the show command options and explanations of output fields, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release.

This is an example of output from the **show vlan** privileged EXEC command, showing all VLANs:

```
Switch# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Gi0/1, Gi0/2
2    VLAN0002                         active    Fa0/12
22   VLAN0022                         active    Fa0/7
102  VLAN0102                         active
200  VLAN0200                         active
222  VLAN0222                         active
400  VLAN0400                         active
1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2005 VLAN2005                         active
2006 VLAN2006                         active
2007 VLAN2007                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
22   enet  100022     1500  -      -      -        -    -        0      0
102  enet  100102     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
222  enet  100222     1500  -      -      -        -    -        0      0
400  enet  100400     1500  -      -      -        -    -        0      0
1000 enet  101000     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   -      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
2005 enet  102005     1500  -      -      -        -    -        0      0
2006 enet  102006     1500  -      -      -        -    -        0      0
2007 enet  102007     1500  -      -      -        -    -        0      0
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0928
3690
Doc.

This is an example of output from the **show vlan brief** privileged EXEC command:

```
Switch# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Gi0/1, Gi0/2
2    VLAN0002                         active    Fa0/12
22   VLAN0022                         active    Fa0/7
102  VLAN0102                         active
200  VLAN0200                         active
222  VLAN0222                         active
400  VLAN0400                         active
1000 VLAN1000                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
2005 VLAN2005                         active
2006 VLAN2006                         active
2007 VLAN2007                         active
```

This is an example of output from the **show running-config vlan** command for a range of VLANs:

```
Switch# show running-config vlan 1005-2005
Building configuration...

Current configuration:
!
vlan 1007
!
vlan 1020
!
vlan 1025
!
vlan 2000
!
vlan 2001
end
```

Configuring VLAN Trunks

These sections describe how VLAN trunks function on the switch:

- Trunking Overview, page 13-18
- 802.1Q Configuration Considerations, page 13-20
- Default Layer 2 Ethernet Interface VLAN Configuration, page 13-21

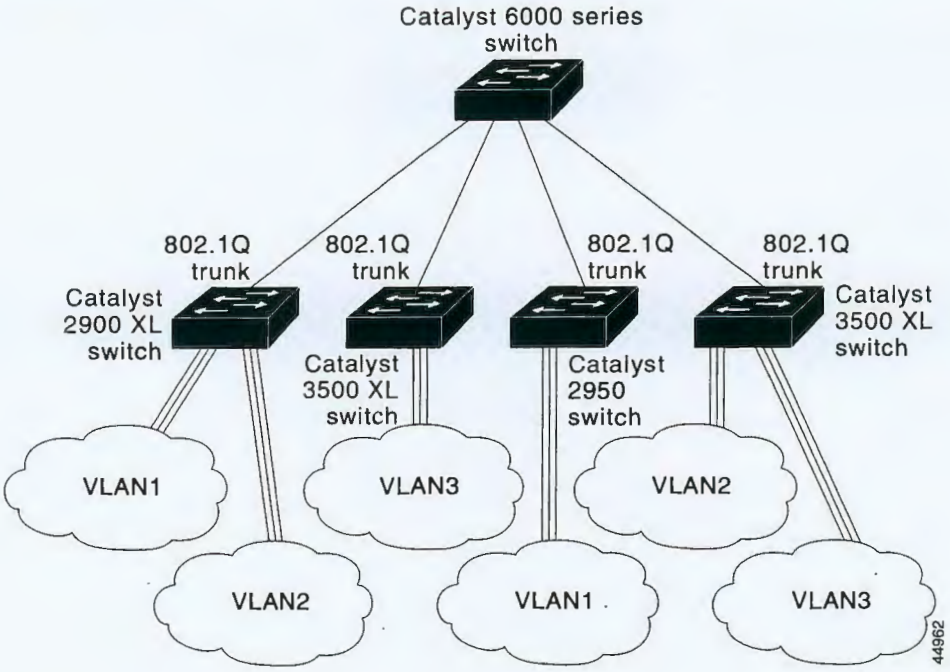
Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Fast Ethernet and Gigabit Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0929
3690
Doc.

Figure 13-2 shows a network of switches that are connected by 802.1Q trunks.

Figure 13-2 Catalyst 2950, 2900 XL, and 3500 XL Switches in a 802.1Q Trunking Environment



You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see Chapter 25, "Configuring EtherChannels."

Ethernet trunk interfaces support different trunking modes (see Table 13-5). You can set an interface a trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol. However, some internetworking devices might forward DTP frames improperly, which coul cause misconfigurations.

To avoid this, you should configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trun but to not generate DTP frames.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3690
Doc.

14-894
A-

Table 13-5 Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface even if the neighboring interface is not a trunk interface.
switchport mode dynamic desirable	Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk*, *desirable*, or *auto* mode. The default switch-port mode for all Ethernet interfaces is **dynamic desirable**.
switchport mode dynamic auto	Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk* or *desirable* mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport nonegotiate	Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is **access** or **trunk**. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

802.1Q Configuration Considerations

802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch to a non-Cisco device through an 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

?OS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0931
3690
Doc.

14.893
CA.

Default Layer 2 Ethernet Interface VLAN Configuration

Table 13-6 shows the default Layer 2 Ethernet interface VLAN configuration.

Table 13-6 Default Layer 2 Ethernet Interface VLAN Configuration

Feature	Default Setting
Interface mode	**switchport mode dynamic desirable**
Allowed VLAN range	VLANs 1–4094 when the enhanced software image is installed and 1 to 1005 when the standard software image is installed
VLAN range eligible for pruning	VLANs 2–1001
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Configuring an Ethernet Interface as a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

This section includes these procedures for configuring an Ethernet interface as a trunk port on the switch:

- Interaction with Other Features, page 13-21
- Defining the Allowed VLANs on a Trunk, page 13-23
- Changing the Pruning-Eligible List, page 13-24
- Configuring the Native VLAN for Untagged Traffic, page 13-25

Note The default mode for Layer 2 interfaces is **switchport mode dynamic desirable**. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk.

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting you entered to all ports in the group:
  - allowed-VLAN list
  - STP port priority for each VLAN
  - STP Port Fast setting
  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0932
Doc. 3690

14.892

- If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as 802.1Q trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface configuration mode and the port to be configured for trunking.
Step 3	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode). • **dynamic auto**—Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. • **dynamic desirable**—Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode. • **trunk**—Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 4	**switchport access vlan** *vlan-id*	(Optional) Specify the default VLAN, which is used if the interface stops trunking.
Step 5	**switchport trunk native vlan** *vlan-id*	Specify the native VLAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport**	Display the switchport configuration of the interface in the *Administrative Mode* and the *Administrative Trunking Encapsulation* fields of the display.
Step 8	**show interfaces** *interface-id* **trunk**	Display the trunk configuration of the interface.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration commands to configure the port as a static-access port.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0933
Doc. 3690

This example shows how to configure the Fast Ethernet interface 0/4 as an 802.1Q trunk and shows several ways to verify the configuration. The example assumes that the neighbor interface is configured to support 802.1Q trunking.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/4
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
Switch# show running-config interface fastethernet0/4
Building configuration...

Current configuration : 112 bytes
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 no ip address
 snmp trap link-status
end

Switch# show interfaces fastethernet0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
```

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094 when the enhanced software image is installed, and 1 to 1005 when the standard software image is installed, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **switchport trunk allowed vlan remove** *vlan-list* interface configuration command to remove specific VLANs from the allowed list.

Note You cannot remove VLAN 1 or VLANs 1002 to 1005 from the allowed-VLAN list.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

RQS nº 03/2005 - CN
CPMI CORREIOS
0934
Fls. Nº
Doc. 3690

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the port to be configured.
Step 3	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 4	**switchport trunk allowed vlan** {**add** | **except** | **none** | **remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, **except**, **none**, and **remove** keywords, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default. You cannot remove any of the default VLANs (1 or 1002 to 1005) from a trunk.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking VLANs Enabled* field of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
Switch#
```

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect. The "Enabling VTP Pruning" section on page 14-14 describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and select the trunk port for which VLANs should be pruned.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0935
Fls. Nº
Doc. 3690

	Command	Purpose
Step 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	Configure the list of VLANs allowed to be pruned from the trunk. (See the "VTP Pruning" section on page 14-4). For explanations about using the **add**, **except**, **none**, and **remove** keywords, refer to the *Catalyst 2950 Desktop Switch Command Reference* for this release. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Pruning VLANs Enabled* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default pruning-eligible list of all VLANs, use the **no switchport trunk pruning vlan** interface configuration command.

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Note The native VLAN can be assigned any VLAN ID; it is not dependent on the management VLAN.

For information about 802.1Q configuration issues, see the "802.1Q Configuration Considerations" section on page 13-20.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and define the interface that is configured as the 802.1Q trunk.
Step 3	**switchport trunk native vlan** *vlan-id*	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094 when the enhanced software image is installed, and 1 to 1005 when the standard software image is installed. Do not enter leading zeros.
Step 4	**end**	Return to privileged EXEC mode.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0096
Doc. 3690

	Command	Purpose
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Trunking Native Mode VLAN* field.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches. For more information about STP, see Chapter 10, "Configuring STP."

Load Sharing Using STP Port Priorities

When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

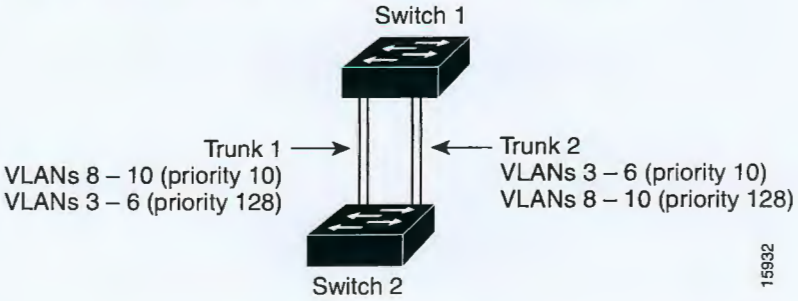
Figure 13-3 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 10 on Trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on Trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2.

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0937
Doc. 3690

Figure 13-3 Load Sharing by Using STP Port Priorities



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 13-3.

	Command	Purpose
Step 1	**vlan database**	On Switch 1, enter VLAN configuration mode.
Step 2	**vtp domain** *domain-name*	Configure a VTP administrative domain. The domain name can be from 1 to 32 characters.
Step 3	**vtp server**	Configure Switch 1 as the VTP server.
Step 4	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 5	**show vtp status**	Verify the VTP configuration on both Switch 1 and Switch 2. In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.
Step 6	**show vlan**	Verify that the VLANs exist in the database on Switch 1.
Step 7	**configure terminal**	Enter global configuration mode.
Step 8	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.
Step 9	**switchport mode trunk**	Configure the port as a trunk port.
Step 10	**end**	Return to privilege EXEC mode.
Step 11	**show interfaces fastethernet0/1 switchport**	Verify the VLAN configuration.
Step 12		Repeat Steps 7 through 11 on Switch 1 for Fast Ethernet port 0/2.
Step 13		Repeat Steps 7 through 11 on Switch 2 to configure the trunk ports on Fast Ethernet ports 0/1 and 0/2.
Step 14	**show vlan**	When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify that Switch 2 has learned the VLAN configuration.
Step 15	**configure terminal**	Enter global configuration mode on Switch 1.
Step 16	**interface fastethernet0/1**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 17	**spanning-tree vlan 8 port-priority 10**	Assign the port priority of 10 for VLAN 8.
Step 18	**spanning-tree vlan 9 port-priority 10**	Assign the port priority of 10 for VLAN 9.
Step 19	**spanning-tree vlan 10 port-priority 10**	Assign the port priority of 10 for VLAN 10.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0938
Doc. 3690

14386
A.

	Command	Purpose
Step 20	**exit**	Return to global configuration mode.
Step 21	**interface fastethernet0/2**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 22	**spanning-tree vlan 3 port-priority 10**	Assign the port priority of 10 for VLAN 3.
Step 23	**spanning-tree vlan 4 port-priority 10**	Assign the port priority of 10 for VLAN 4.
Step 24	**spanning-tree vlan 5 port-priority 10**	Assign the port priority of 10 for VLAN 5.
Step 25	**spanning-tree vlan 6 port-priority 10**	Assign the port priority of 10 for VLAN 6.
Step 26	**end**	Return to privileged EXEC mode.
Step 27	**show running-config**	Verify your entries.
Step 28	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

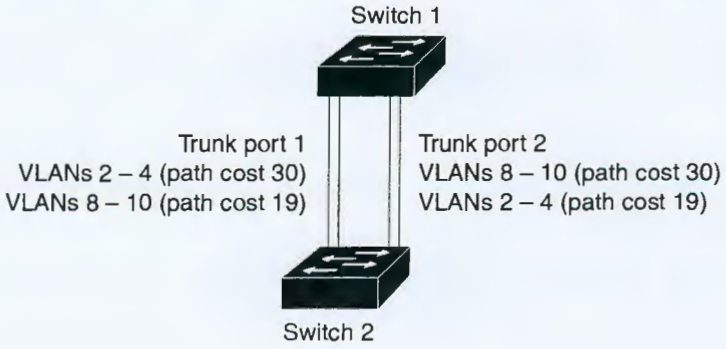
Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs. The VLANs keep the traffic separate. Because no loops exist, STP does not disable the ports, and redundancy is maintained in the event of a lost link.

In Figure 13-4, Trunk ports 1 and 2 are 100BASE-T ports. The path costs for the VLANs are assigned as follows:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1.
- VLANs 8 through 10 retain the default 100BASE-T path cost on Trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2.
- VLANs 2 through 4 retain the default 100BASE-T path cost on Trunk port 2 of 19.

Figure 13-4 Load-Sharing Trunks with Traffic Distributed by Path Cost



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 929
Doc. 3690

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 13-4:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch 1.
Step 2	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to be configured as a trunk.

	Command	Purpose
Step 3	**switchport mode trunk**	Configure the port as a trunk port.
Step 4	**exit**	Return to global configuration mode.
Step 5		Repeat Steps 2 through 4 on Switch 1 interface Fast Ethernet 0/2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries. In the display, make sure that interfaces Fast Ethernet 0/1 and Fast Ethernet 0/2 are configured as trunk ports.
Step 8	**show vlan**	When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration.
Step 9	**configure terminal**	Enter global configuration mode.
Step 10	**interface fastethernet 0/1**	Enter interface configuration mode, and define Fast Ethernet port 0/1 as the interface to set the STP cost.
Step 11	**spanning-tree vlan 2 cost 30**	Set the spanning-tree path cost to 30 for VLAN 2.
Step 12	**spanning-tree vlan 3 cost 30**	Set the spanning-tree path cost to 30 for VLAN 3.
Step 13	**spanning-tree vlan 4 cost 30**	Set the spanning-tree path cost to 30 for VLAN 4.
Step 14	**end**	Return to global configuration mode.
Step 15		Repeat Steps 9 through 11 on Switch 1 interface Fast Ethernet 0/2, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.
Step 16	**exit**	Return to privileged EXEC mode.
Step 17	**show running-config**	Verify your entries. In the display, verify that the path costs are set correctly for interfaces Fast Ethernet 0/1 and 0/2.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0940
Doc. 3690

Configuring VMPS

The Catalyst 2950 switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through the VLAN Query Protocol (VQP). VMPS dynamically assigns dynamic access port VLAN membership.

This section includes this information about configuring VMPS:

- "Understanding VMPS" section on page 13-30
- "Default VMPS Configuration" section on page 13-33
- "VMPS Configuration Guidelines" section on page 13-33
- "Configuring the VMPS Client" section on page 13-34
- "Monitoring the VMPS" section on page 13-36
- "Troubleshooting Dynamic Port VLAN Membership" section on page 13-37
- "VMPS Configuration Example" section on page 13-37

Understanding VMPS

When the VMPS receives a VQP request from a client switch, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in secure mode. Secure mode determines whether the server shuts down the port when a VLAN is not allowed on it or just denies the port access to the VLAN.

In response to a request, the VMPS takes one of these actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:
  - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.
  - If the VLAN is not allowed on the port and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.
  - If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch receives an *access-denied* response from the VMPS, it continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI, CMS, or SNMP.

You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response, depending on the VMPS secure mode setting.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0941
Doc. 3690

Dynamic Port VLAN Membership

A dynamic (nontrunking) port on the switch can belong to only one VLAN, with a VLAN ID from 1 to 1005. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN; however, the VMPS shuts down a dynamic port if more than 20 hosts are active on the port.

If the link goes down on a dynamic port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

VMPS Database Configuration File

The VMPS contains a database configuration file that you create. This ASCII text file is stored on a switch-accessible TFTP server that functions as a VMPS server. The file contains VMPS information, such as the domain name, the fallback VLAN name, and the MAC-address-to-VLAN mapping. The Catalyst 2950 switch cannot act as the VMPS, but you can use a Catalyst 5000 or Catalyst 6000 series switch as the VMPS.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

Whenever port names are used in the VMPS database configuration file, the server must use the switch convention for naming ports. For example, Fa0/4 is fixed Fast Ethernet port number 4. If the switch is a cluster member, the command switch adds the name of the switch before the type. For example, *es3%Fa0/4* refers to fixed Fast Ethernet port 4 on member switch 3. When port names are required, these naming conventions must be followed in the VMPS database configuration file when it is configured to support a cluster.

This example shows a example of a VMPS database configuration file as it appears on a Catalyst 6000 series switch. The file has these characteristics:

- The security mode is open.
- The default is used for the fallback VLAN.
- MAC address-to-VLAN name mappings—The MAC address of each host and the VLAN to which each host belongs is defined.
- Port groups are defined.
- VLAN groups are defined.
- VLAN port policies are defined for the ports associated with restricted VLANs.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0942
Doc. 3690

```
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain DSBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
 device 198.92.30.32 port 0/2
 device 172.20.26.141 port 0/8
vmps-port-group "Executive Row"
 device 198.4.254.222 port 0/2
 device 198.4.254.222 port 0/3
 device 198.4.254.223 all-ports
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
 port-group WiringCloset1
vmps-port-policies vlan-name Green
 device 198.92.30.32 port 0/8
```

14.882
MP 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0943
Doc: 3690

```
vmps-port-policies vlan-name Purple
 device 198.4.254.22 port 0/2
 port-group "Executive Row"
```

Default VMPS Configuration

Table 13-7 shows the default VMPS and dynamic port configuration on client switches.

Table 13-7 Default VMPS Client and Dynamic Port Configuration

Feature	Default Setting
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic ports	None configured

VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic port VLAN membership:

- You must configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. For the cluster-based port-naming conventions, see the "VMPS Database Configuration File" section on page 13-31.
- When you configure a port as dynamic, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state. You can disable Port Fast mode on a dynamic port.
- 802.1X ports cannot be configured as dynamic ports. If you try to enable 802.1X on a dynamic-access (VQP) port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic access setting takes effect.
- Dynamic ports cannot be network ports or monitor ports.
- Secure ports cannot be dynamic ports. You must disable port security on a port before it becomes dynamic.
- Dynamic ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic ports.
- The VTP management domain of the VMPS client and the VMPS server must be the same.
- VQP does not support extended-range VLANs (VLAN IDs higher than 1006). Extended-range VLANs cannot be configured by VMPS.
- The VLAN configured on the VMPS server should not be a voice VLAN.

POS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0944
3690
Doc.

14-380 A.

Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch can be a VMPS client; it cannot be a VMPS server.

Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch as a client.

Note If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps server** *ipaddress* **primary**	Enter the IP address of the switch acting as the primary VMPS server.
Step 3	**vmps server** *ipaddress*	Enter the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vmps**	Verify your entries in the *VMPS Domain Server* field of the display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note The switch port that is connected to the VMPS server cannot be a dynamic access port. It can be either a static access port or a trunk port. See the "Configuring an Ethernet Interface as a Trunk Port" section on page 13-21.

Configuring Dynamic Access Ports on VMPS Clients

If you are configuring a port on a cluster member switch as a dynamic port, first use the **rcommand** privileged EXEC command to log into the member switch.

Caution Dynamic port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic access ports to other switches can cause a loss of connectivity.

Beginning in privileged EXEC mode, follow these steps to configure a dynamic access port on a VMPS client switch:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the switch port that is connected to the end station.
Step 3	**switchport mode access**	Set the port to access mode.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0945
Fls. Nº
Doc: 3690

	Command	Purpose
Step 4	**switchport access vlan dynamic**	Configure the port as eligible for dynamic VLAN membership. The dynamic access port must be connected to an end station.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Operational Mode* field of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To return an interface to its default switchport mode (dynamic desirable), use the **no switchport mode** interface configuration command. To reset the access mode to the default VLAN for the switch, use the **no switchport access** interface configuration command.

Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic port VLAN membership assignments that the switch has received from the VMPS:

	Command	Purpose
Step 1	**vmps reconfirm**	Reconfirm dynamic port VLAN membership.
Step 2	**show vmps**	Verify the dynamic VLAN reconfirmation status.

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch. You must also first use the **rcommand** privileged EXEC command to log into the member switch.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps reconfirm** *minutes*	Enter the number of minutes between reconfirmations of the dynamic VLAN membership. Enter a number from 1 to 120. The default is 60 minutes.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps reconfirm** global configuration command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0340
Fls. Nº 13-35
3690
Doc:

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps retry** *count*	Change the retry count. The retry range is from 1 to 10; the default is 3.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify your entry in the *Server Retry Count* field of the display.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no vmps retry** global configuration command.

Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The switch displays this information about the VMPS:

VMPS VQP Version — The version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP version 1.

Reconfirm Interval — The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.

Server Retry Count — The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.

VMPS domain server — The IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked *current*. The one marked *primary* is the primary server.

VMPS Action — The result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expired, or you can force it by entering the **vmps reconfirm** privileged EXEC command or its CMS or SNMP equivalent.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1617
Doc: 3690

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps

VQP Client Status:
--------------------
VMPS VQP Version:    1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:          No Dynamic Port
```

Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic port.

To re-enable a disabled dynamic port, enter the **no shutdown** interface configuration command.

VMPS Configuration Example

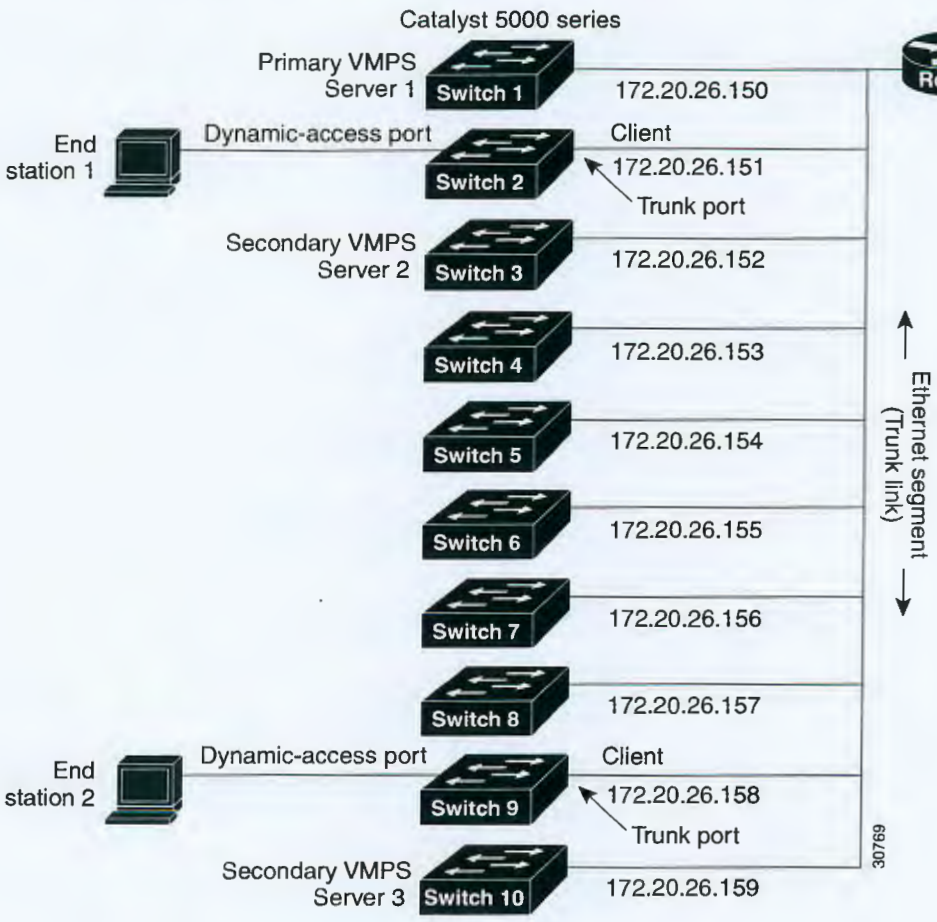
Figure 13-5 shows a network with a VMPS server switch and VMPS client switches with dynamic ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 5000 series Switch 1 is the primary VMPS server.
- The Catalyst 5000 series Switch 3 and Switch 10 are secondary VMPS servers.
- The end stations are connected to these clients:
  - Catalyst 2950 Switch 2
  - Catalyst 3500 XL Switch 9
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

QS nº 0372005 - CN -
CPMI - CORREIOS
0048
Fls. Nº
Doc: 3690

ECT 14.876 A. CPMI - C

Figure 13-5 Dynamic Port VLAN Membership Configuration



...s nº 03/2005 - CN -
...MI - CORREIOS
Fls. Nº 0949
3690
Doc:

14.961
A-

Switch Tipo 2 doc 3

PS nº 03/2005 ON -
PMI - CORREIOS
Fls. Nº
Doc: 3690

CHAPTER 2

Installation

This chapter describes how to install your switch, interpret the power-on self-test (POST), and connect the switch to other devices. Read these topics and perform the procedures in this order:

- Preparing for Installation, page 2-2
- Installing the Switch in a Rack, page 2-9
- Installing the Switch on a Table, Shelf, or Desk, page 2-20
- Installing the GBIC Modules, page 2-20
- Powering On the Switch, page 2-22
- Connecting to DC Power, page 2-23
- Running POST, page 2-32
- Connecting to 10/100 and 10/100/1000 Ports, page 2-33
- Connecting to 100BASE-FX and 1000BASE-SX Ports, page 2-37
- Connecting to GBIC Module Ports, page 2-38
- Connecting a PC or a Terminal to the Console Port, page 2-43
- Where to Go Next, page 2-45

14.960
J.A.

...QS nº 03/2005 - CN -
...CORREIOS
Fls. Nº 0951
Doc: 3690

Preparing for Installation

This section provides information about these topics:

- Warnings, page 2-2
- EMC Regulatory Statements, page 2-4
- Installation Guidelines, page 2-6
- Verifying Package Contents, page 2-7

Warnings

These warnings are translated into several languages in Appendix C, "Translated Safety Warnings."

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.**

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Unplug the power cord before you work on a system that does not have an on/off switch.**

Warning **Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0952
3690
Doc:

14.938
A.

Warning The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

Warning To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Warning When installing the unit, always make the ground connection first and disconnect it last.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning Ultimate disposal of this product should be handled according to all national laws and regulations.

Warning Attach only the Cisco RPS (model PWR300-AC-RPS-N1) to the RPS receptacle.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 2-3
Doc: 3690

14957
A

Warning **Class 1 laser product**

Warning **Avoid exposure to the laser beam.**

EMC Regulatory Statements

This section includes specific regulatory statements about the Catalyst 2950 switches.

U.S.A.

U.S. regulatory information for this product is in the front matter of this manual.

Taiwan

This is a Class A Information product. When used in a residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. N 0954
Doc: 3690

14 956
A

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

46464

Korea

Warning **This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type.**

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

RQS nº 03/2005 - CN - CORREIOS
0955
Fls. Nº
Doc: 3690

14.955
A-

Hungary

This equipment is a Class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

Figyelmeztetés a felhasználói kézikönyv számára:
Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleloen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Installation Guidelines

When determining where to place the switch, observe these guidelines.

- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- For 100BASE-FX ports, the cable length from a switch to an attached device cannot exceed 6562 feet (2 kilometers).
- For 1000BASE-SX ports and 1000BASE-SX GBIC module ports, the cable length from a switch to an attached device cannot exceed 1804 feet (550 meters).
- For 1000BASE-LX/LH GBIC module ports, the cable length from a switch to an attached device cannot exceed 32,810 feet (10 kilometers).
- For 1000BASE-ZX GBIC module ports, the cable length from a switch to an attached device cannot exceed 328,100 feet (100 kilometers).
- For 1000BASE-T GBIC module ports, the cable length from switch to an attached device cannot exceed 328 feet (100 meters).
- For Coarse Wave Division Multiplexing (CWDM) GBIC module ports, the cable length from a switch to an attached device cannot exceed 393,719 feet (120 kilometers). For specific cable lengths, refer to the CWDM GBIC module documentation.
- For GigaStack GBIC module ports, the cable length from a switch to an attached device cannot exceed 3 feet (1 meter).

ECOS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0956
Doc: 3690

- Operating environment is within the ranges listed in Appendix A, "Technical Specifications."
- Clearance to front and rear panels meet these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Rear-panel AC power connector is within reach of an AC power outlet.
  - Rear-panel direct current (DC) power connector is within reach of a circuit breaker.
- Airflow around the switch and through the vents is unrestricted.
- Temperature around the unit does not exceed 113°F (45°C).

Note If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.

Verifying Package Contents

Note Carefully remove the contents from the shipping container, and check each item for damage. If any item is missing or damaged, contact your Cisco representative or reseller for support. Return all packing materials to the shipping container and save them.

The switch is shipped with these items:

- This *Catalyst 2950 Desktop Switch Hardware Installation Guide*
- *Where to Find the Catalyst 2950 Documentation* flyer
- Cisco Documentation CD-ROM
- AC power cord

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0957
Doc: 3690
12-7

- Mounting kit containing these items:
  - Four rubber feet for mounting the switch on a table, shelf, or desk
  - Two 19-inch or 24-inch rack-mounting brackets
  - Six number-8 Phillips flat-head screws for attaching the brackets to the switch
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Four number-12 Phillips machine screws for attaching the brackets to a rack
  - One cable guide and one black Phillips machine screw for attaching the cable guide to one of the mounting brackets
- DC-switch kit containing these items:
  - One DC terminal block plug (also called a terminal block header)
  - One ground lug
  - Two number-10-32 screws for attaching the ground lug to the switch
  - Two 23-inch rack-mounting brackets (with 1-inch spacing for telco racks)
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Two number-12 Phillips machine screws for attaching the brackets to a rack

Note The DC-switch kit ships only with the Catalyst 2950G-24-EI-DC switch.

- One RJ-45-to-DB-9 adapter cable
- Cisco Information Packet, containing safety and support information

If you want to connect a terminal to the switch console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0958
Fls. Nº
3690
Doc:

14.951
A

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on a target device by using one of the MT-RJ fiber-optic patch cables listed in Table 2-1. Use the Cisco part numbers in Table 2-1 to order the patch cables that you need.

Table 2-1 MT-RJ Patch Cables for 100BASE-FX and 1000BASE-SX Connections

Type	Cisco Part Number
1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

Installing the Switch in a Rack

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Note Figure 2-1 to Figure 2-17 show the Catalyst 2950-24, 2950G-24-EI-DC, and 2950G-48-EI switches as examples. You can install other Catalyst 2950 switches in a rack as shown in these illustrations.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0959
Fls. Nº 2-9
Doc: 3690

14.951
A.

To install the switch in a 19-, 23-, or 24-inch rack, follow these steps:

- Attaching the Brackets to the Switch, page 2-10
- Mounting the Switch in a Rack, page 2-19
- Attaching the Optional Cable Guide, page 2-19

Note Installing the Catalyst 2950G-48-EI switch in a 23-inch or 24-inch rack requires an optional bracket kit not included with the switch. You can order a kit containing the 23-inch or 24-inch rack-mounting brackets and hardware from Cisco (part number RCKMNT-1RU=).

Attaching the Brackets to the Switch

The bracket orientation and the screws that you use depend on whether you are attaching the brackets to a 19-, 23-, or 24-inch rack. Follow these guidelines:

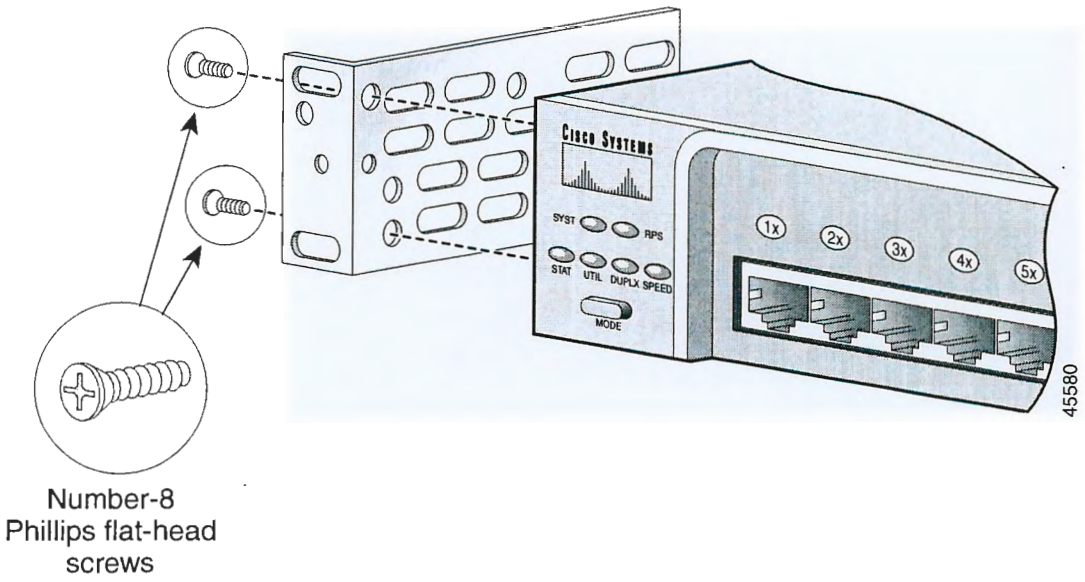
- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 19-inch rack, use two Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 2-1, Figure 2-2, and Figure 2-3.
- When mounting a Catalyst 2950G-48-EI switch in a 19-inch rack, use three Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 2-4, Figure 2-5, and Figure 2-6.
- When mounting a Catalyst 2950G-24-EI-DC switch in a 23-inch rack, use two Phillips truss-head screws to attach the 23-inch bracket to the switch. See Figure 2-7, Figure 2-8, and Figure 2-9.
- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 24-inch rack, use two Phillips truss-head screws to attach the 19- or 24-inch bracket to the switch. See Figure 2-10, Figure 2-11, and Figure 2-12.
- When mounting a Catalyst 2950G-48-EI switch in a 24-inch rack, use three Phillips flat-head screws to attach the 24-inch bracket (part number RCKMNT-1RU=) to the switch. See Figure 2-13, Figure 2-14, and Figure 2-15.

Figure 2-1 to Figure 2-15 show how to attach a bracket to one side of the switch. Follow the same steps to attach the second bracket to the opposite side of the switch.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0960
Doc 3690

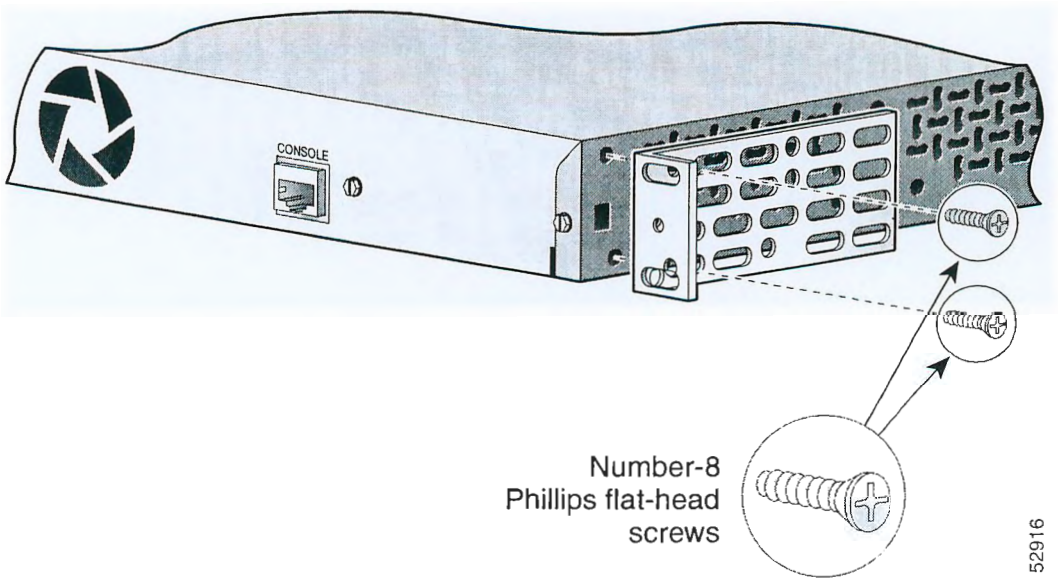
14.950
A.

Figure 2-1 Attaching Brackets on the Switch in a 19-Inch Rack (Front Panel Forward)



Number-8
Phillips flat-head
screws

Figure 2-2 Attaching Brackets on the Switch in a 19-Inch Rack (Rear Panel Forward)



Number-8
Phillips flat-head
screws

BOS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0961
Doc: 3690

14349
A.

Figure 2-3 Attaching Brackets on the Switch in a 19-Inch Telco Rack

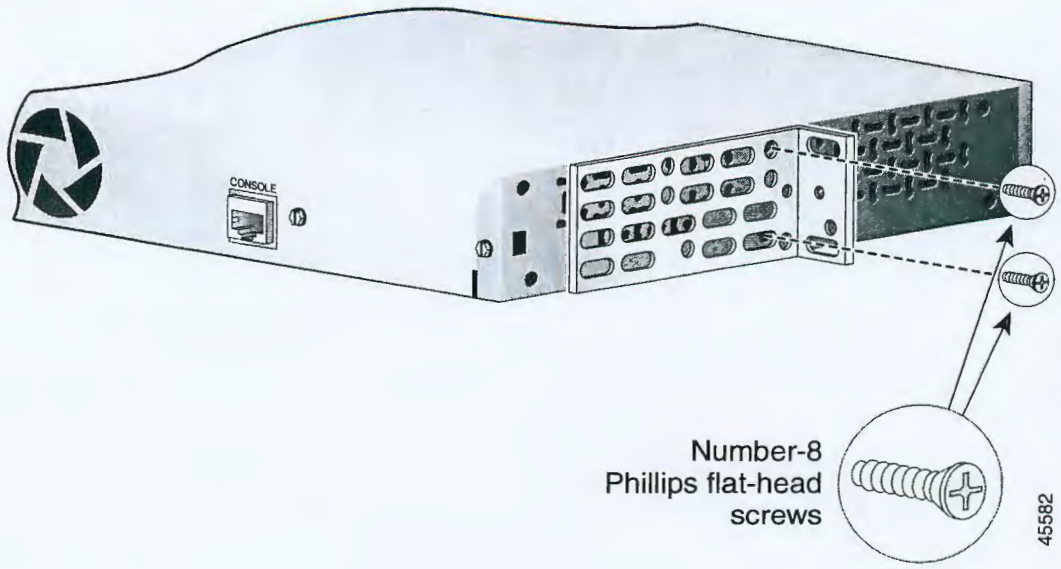
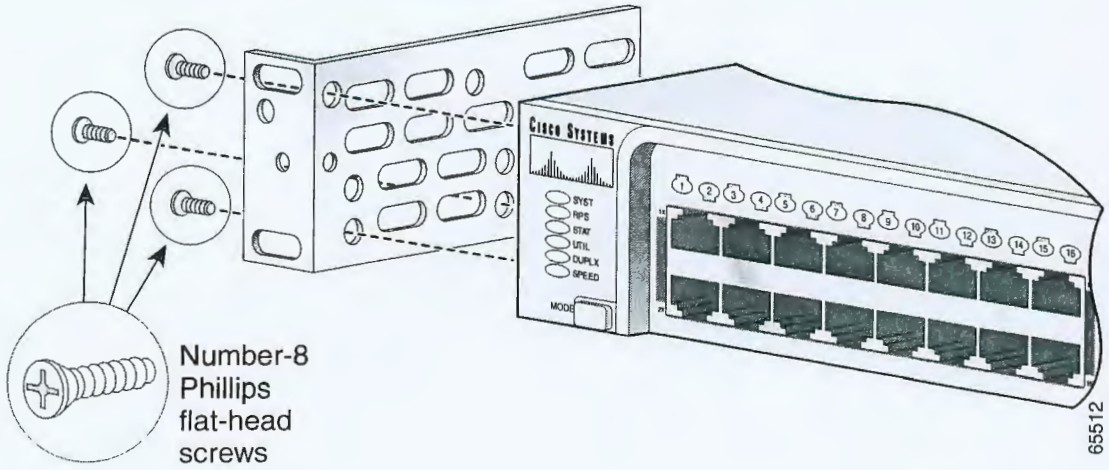


Figure 2-4 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Front Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
0962
Fls. Nº
78-11157-03
3690
Doc:

14.948
A.

Figure 2-5 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Rear Panel Forward)

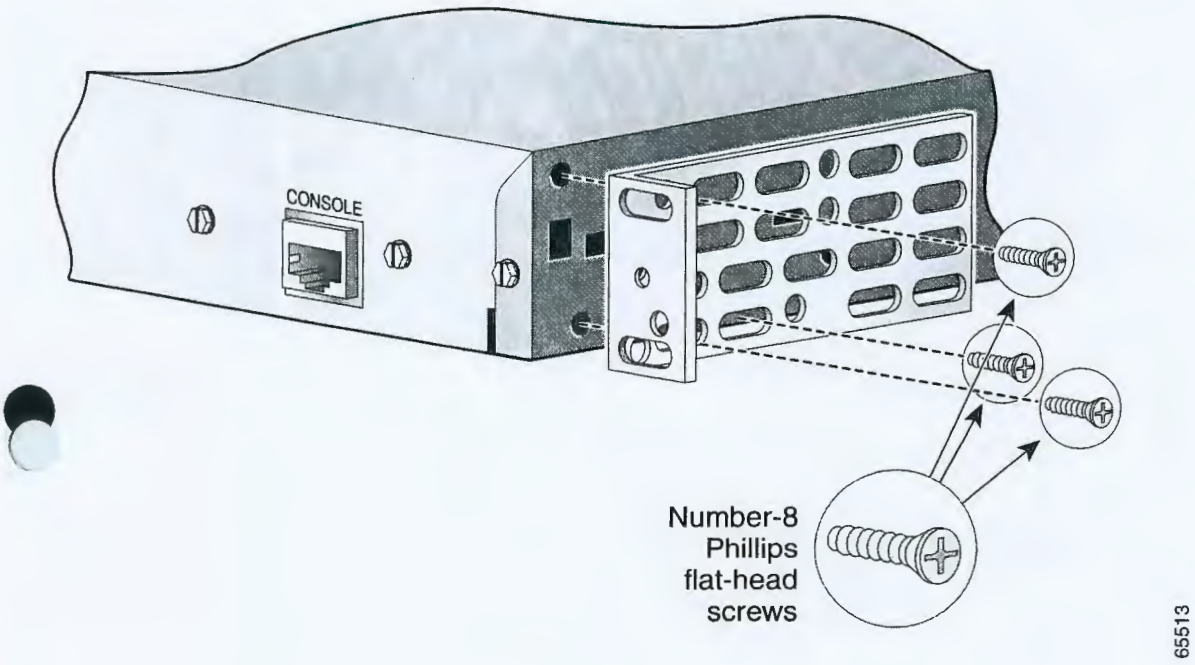
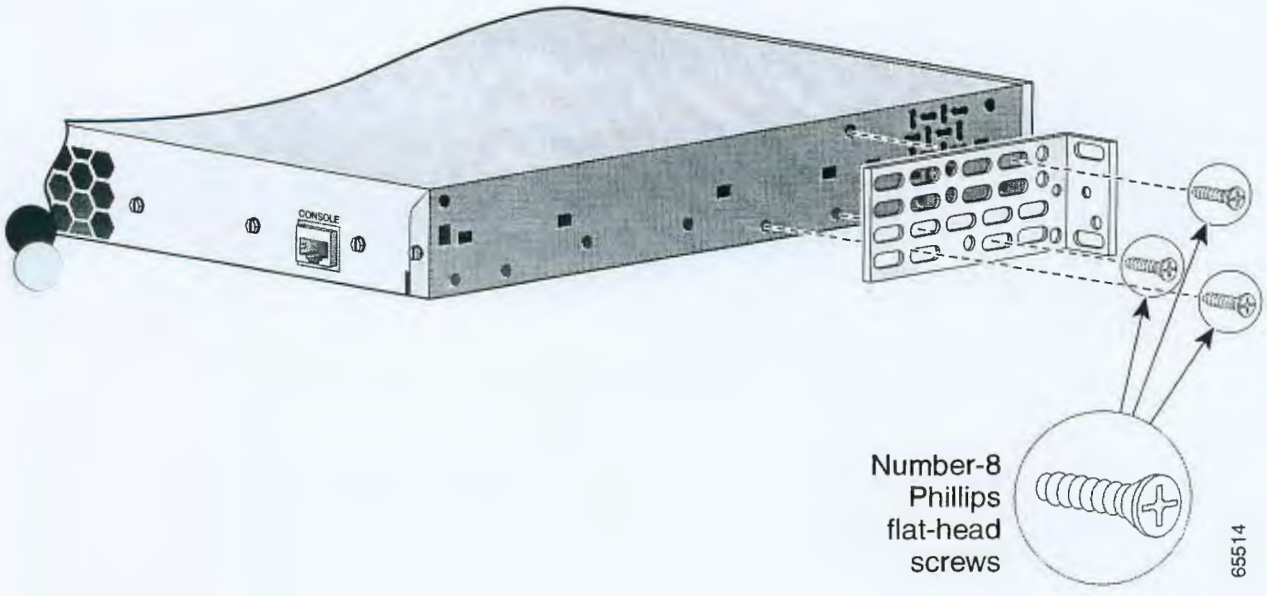


Figure 2-6 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Telco Rack



POS nº 03/2005 - CN -
CORREIOS
Fls. Nº 0963
Doc: 3690

Figure 2-7 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack (Front Panel Forward)

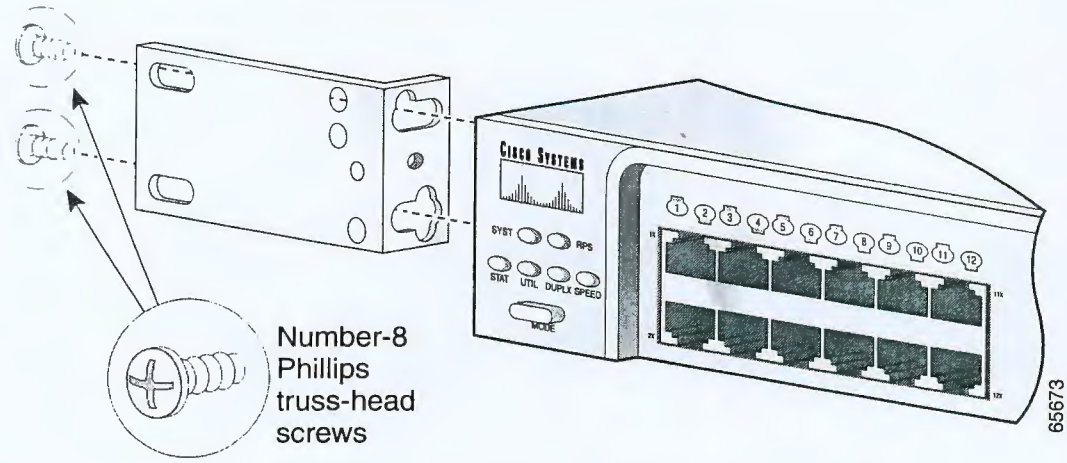
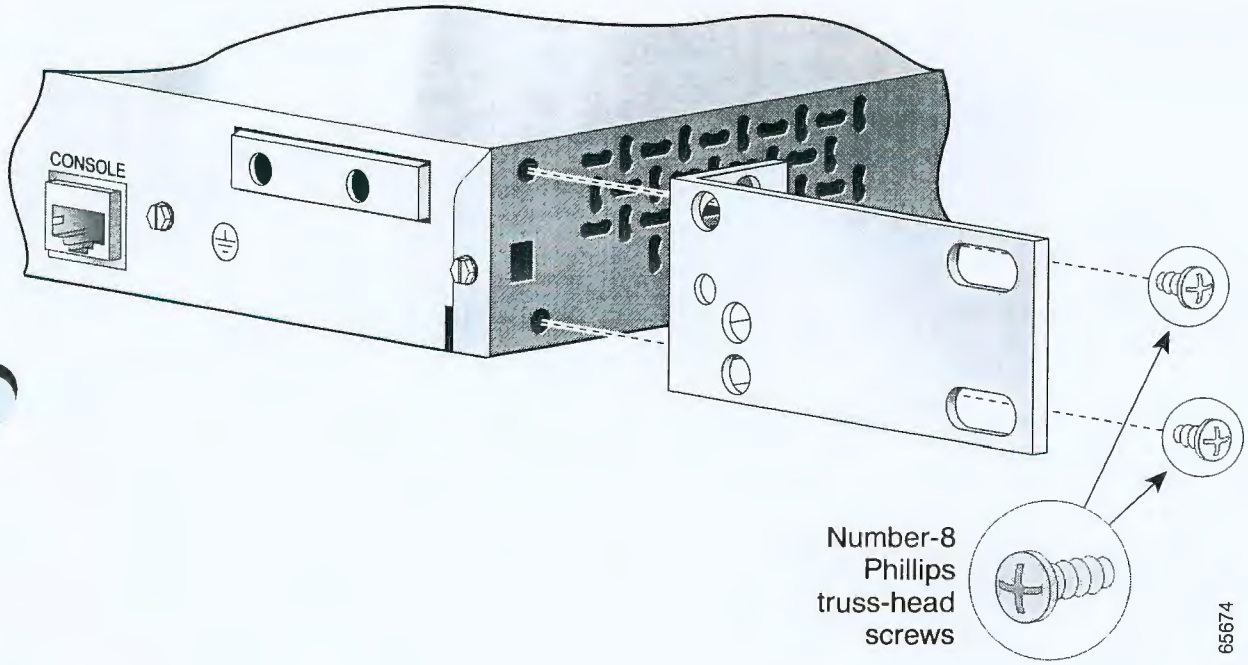


Figure 2-8 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack (Rear Panel Forward)



...OS nº 03/2005 - CN -
...PMI - CORREIOS
0964
Fls. Nº
3690
Doc:

Figure 2-9 Attaching Brackets on the Catalyst 2950G-24-EI-DC Switch in a 23-Inch Telco Rack

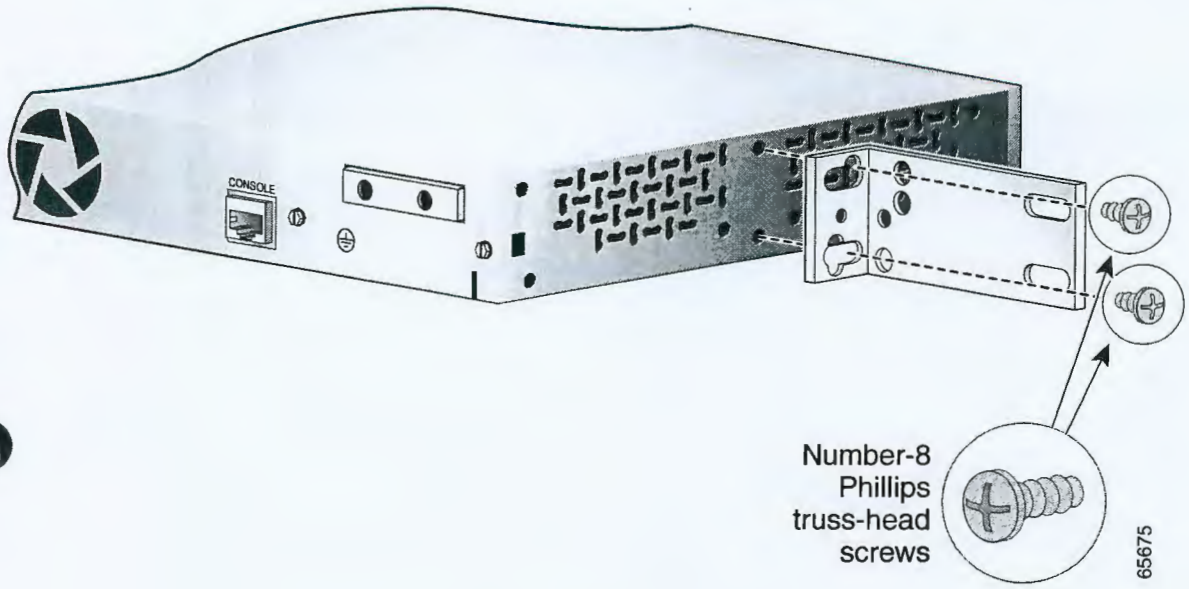
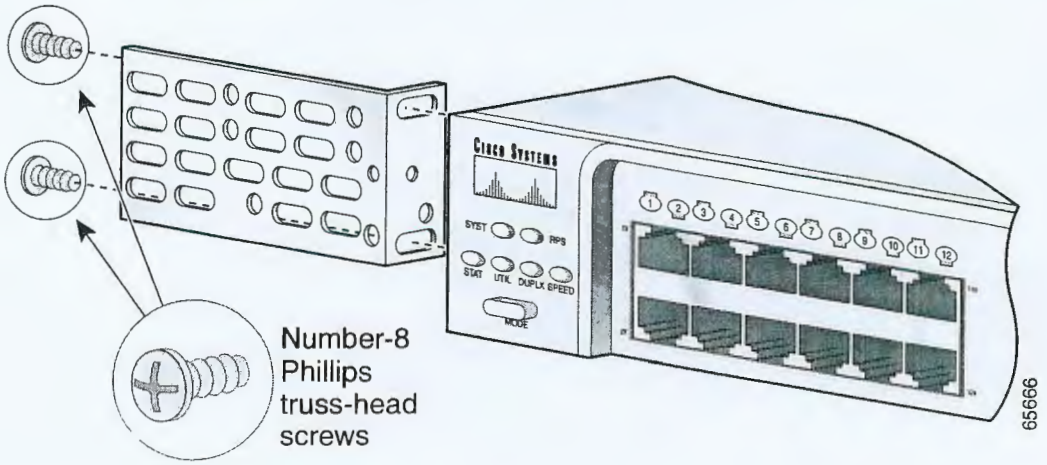


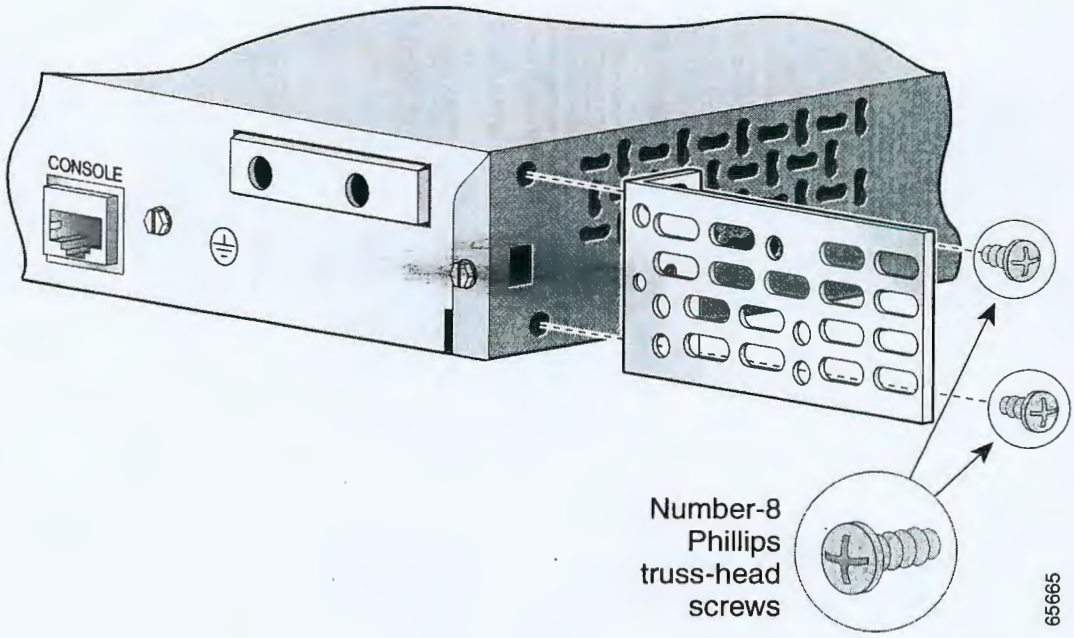
Figure 2-10 Attaching Brackets on the Switch in a 24-Inch Rack (Front Panel Forward)



ECS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0965
Doc: 3690

14.945
VA

Figure 2-11 Attaching Brackets on the Switch in a 24-Inch Rack (Rear Panel Forward)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0966
Doc: 3690

14.944
SA.

Figure 2-12 Attaching Brackets on the Switch in a 24-Inch Telco Rack

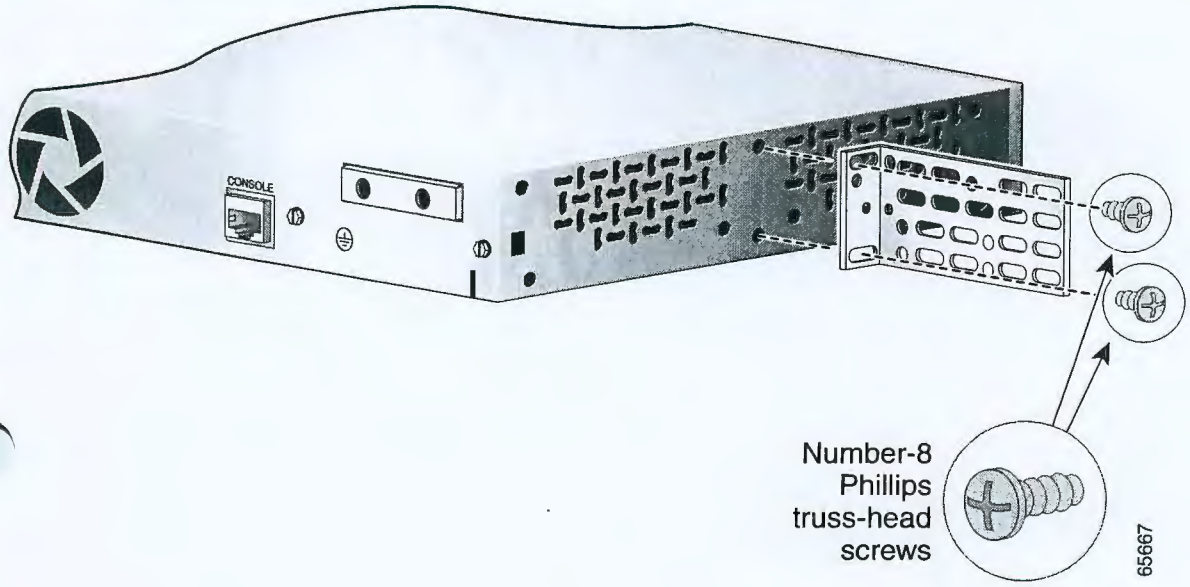
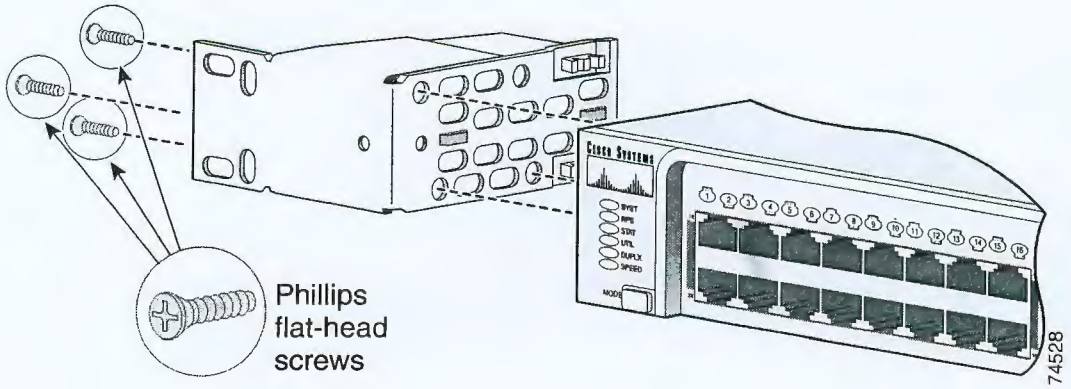


Figure 2-13 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Front Panel Forward)



ROS nº 03/2005 - CN -
SPMI - CORREIOS
Fls. Nº 0967
Doc: 3690

14.943
A-

Figure 2-14 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Rear Panel Forward)

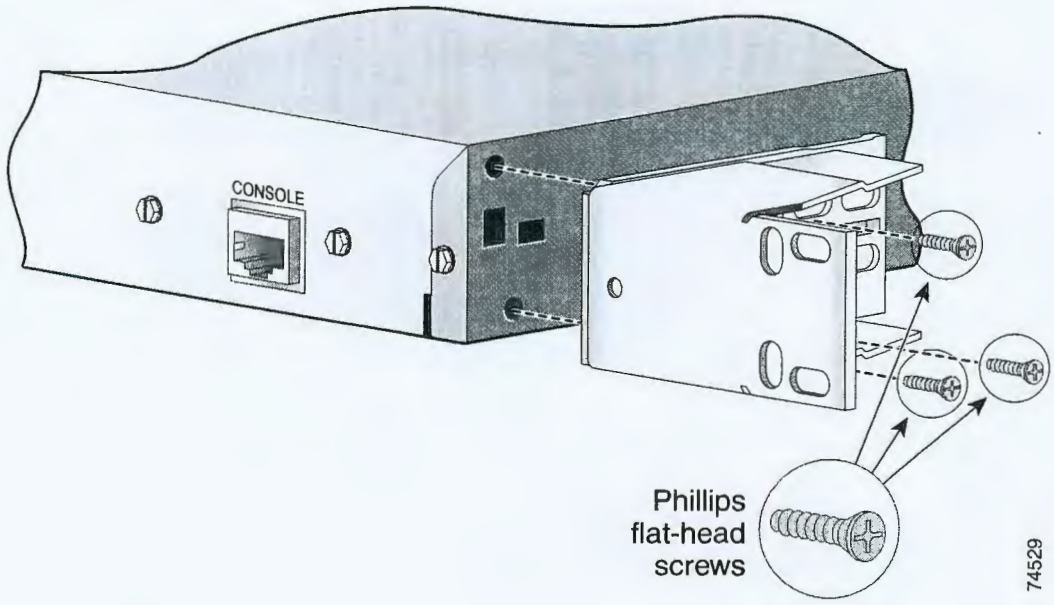
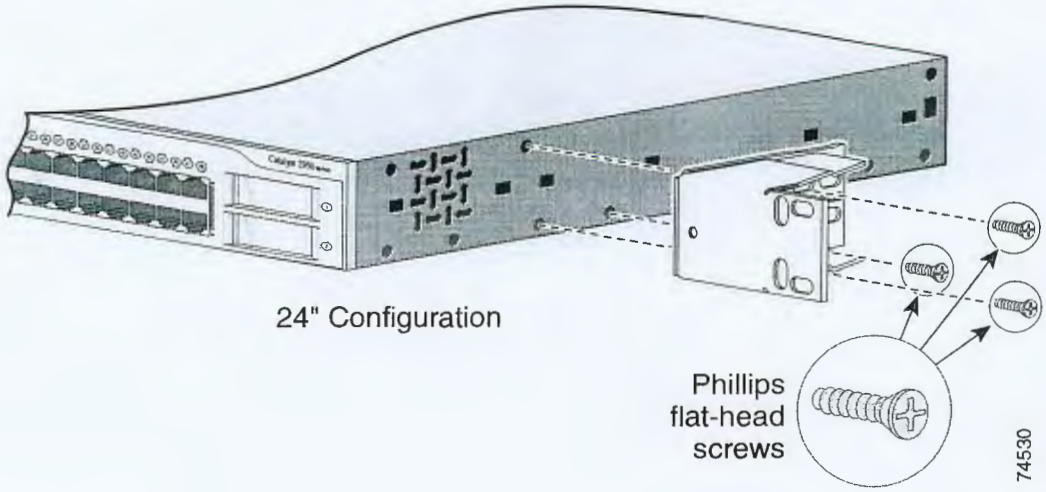


Figure 2-15 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Telco Rack



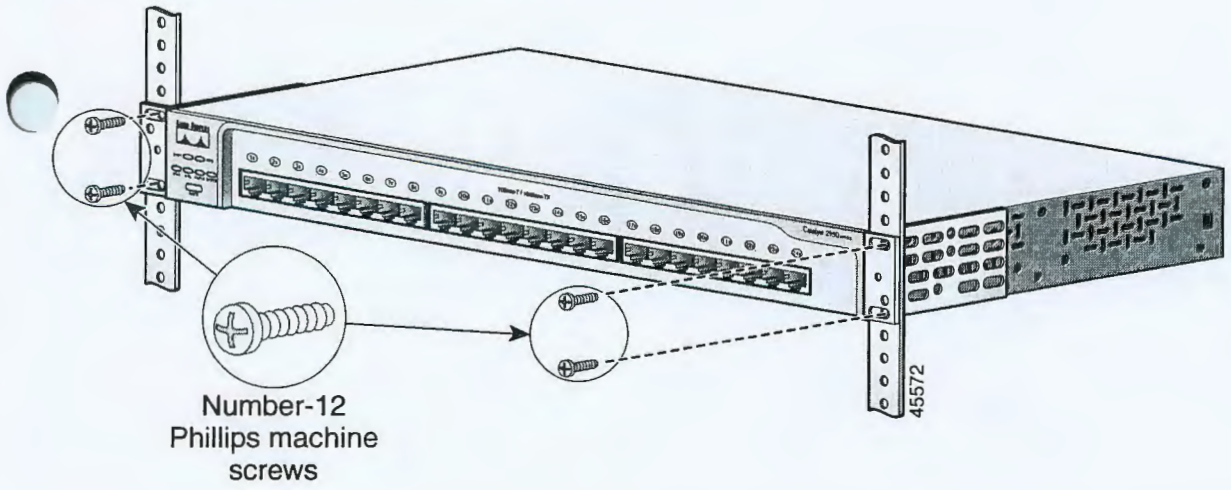
03/2005 - CN -
CORREIOS
Fls. Nº 1978
Doc: 3690

Mounting the Switch in a Rack

After attaching the brackets, use the four Phillips machine screws to securely attach the brackets to the rack, as shown in Figure 2-16.

To prevent the cables from obscuring the switch and other devices in the rack, you can also attach the cable guide to the rack. See the"Attaching the Optional Cable Guide" section for instructions.

Figure 2-16 Mounting the Switch in a Rack



After mounting the switch in the rack, start the terminal-emulation software, and provide power to the switch. See the "Powering On the Switch" section on page 2-22 for instructions.

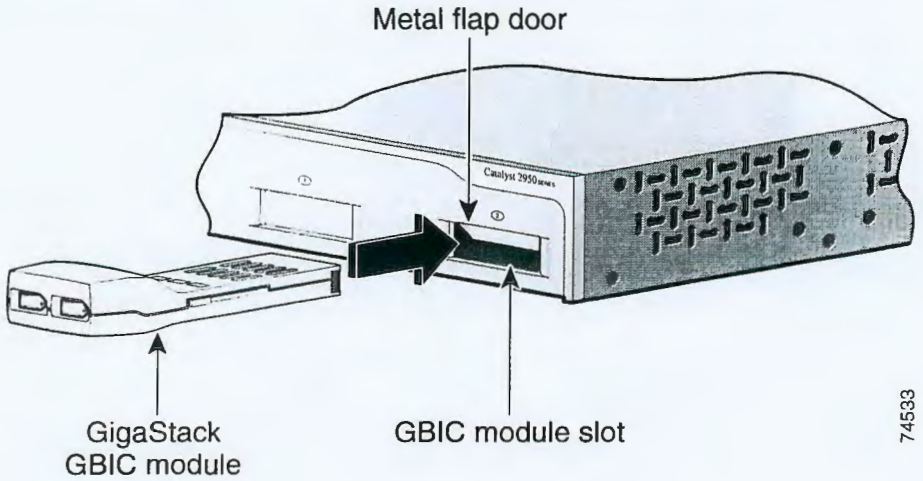
Attaching the Optional Cable Guide

We recommend attaching the cable guide to prevent the cables from obscuring the front panels of the switch and other devices installed in the rack. Use the supplied black Phillips machine screw to attach the cable guide to the left or right bracket, as shown in Figure 2-17.

IQS nº 03/2005 - CN -
CORREIOS
Fls. Nº 0969
3690
Doc:

34.939
A.

Figure 2-20 Installing a GigaStack GBIC Module in a Switch



Powering On the Switch

Before connecting the AC power cord, a DC-input power source, or the Redundant Power System (RPS) to the switch, make sure that you have started the terminal-emulation software (such as ProComm, HyperTerminal, tip, or minicom) from your management station.

If you are using the AC power cord, connect the AC power cord to the AC power connector and to an AC power outlet.

If you are using the DC-input power source, see the "Connecting to DC Power" section for installation instructions.

If you are using an RPS, refer to the documentation that came with your RPS for installation instructions.

Warning **Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle.**

For POST information, see the "Running POST" section on page 2-32.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0970
Fls. Nº
3690
Doc:

Connecting to DC Power

To connect the Catalyst 2950G-24-EI-DC switch to a DC-input power source, follow these steps:

- Preparing for Installation, page 2-23
- Grounding the Switch, page 2-24
- Wiring the DC-Input Power Source, page 2-26

Warning **The Catalyst 2950G-24-EI-DC contains no field-replaceable units (FRUs). Do not open the chassis or attempt to remove or replace any components. For information about obtaining service for this unit, contact your reseller or Cisco sales representative.**

Warning **The equipment is to be installed in a restricted access area.**

Warning **Ethernet cables must be shielded when used in a central office environment.**

Preparing for Installation

Locate the DC terminal block plug, the ground lug, and the two number-10-32 screws in the DC-switch kit.

Obtain these necessary tools and equipment:

- Ratcheting torque screwdriver with a Phillips head that exerts up to 15 pound-force inches (lbf-in.) of pressure
- Panduit crimping tool with optional controlled cycle mechanism (model CT-700, CT-720, CT-920, CT-920CH, CT-930, or CT-940CH)
- 6-gauge copper ground wire (insulated or noninsulated)
- Four leads of 18-gauge copper wire
- Wire-stripping tools for stripping 6- and 18-gauge wires

EOS - 03/2005 - CN -
CPMI - CORREIO
Fls. Nº 0971
3690
Doc:

Grounding the Switch

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

Warning **When installing the unit, always make the ground connection first and disconnect it last.**

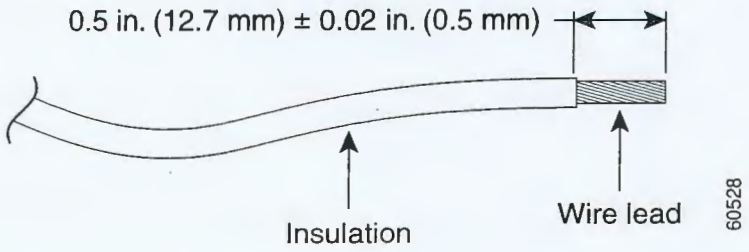
Caution To make sure that the equipment is reliably connected to earth ground, follow the grounding procedure instructions, and use a UL-listed lug suitable for number-6 AWG wire and two number-10-32 ground-lug screws.

To ground the switch to earth ground, follow these steps. Make sure to follow any grounding requirements at your site.

Step 1 Locate the ground lug and the two number-10-32 screws from the switch rear panel. Use a standard Phillips screwdriver or a ratcheting torque screwdriver with a Phillips head. Set the screws and the ground lug aside.

Step 2 If your ground wire is insulated, use a wire stripping tool to strip the 6-gauge ground wire to 0.5 inch (12.7 millimeter [mm]) 0.02 inch (0.5 mm) as shown in Figure 2-21.

Figure 2-21 Stripping the Ground Wire

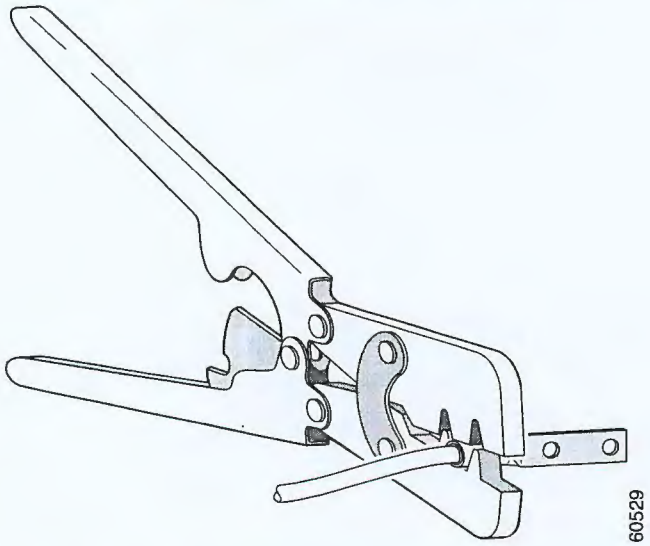


Step 3 Slide the open end of the ground lug over the exposed area of the 6-gauge wire.

ECOS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 172
Doc: 3690

Step 4 Using a Panduit crimping tool, crimp the ground lug to the 6-gauge wire.

Figure 2-22 Crimping the Ground Lug

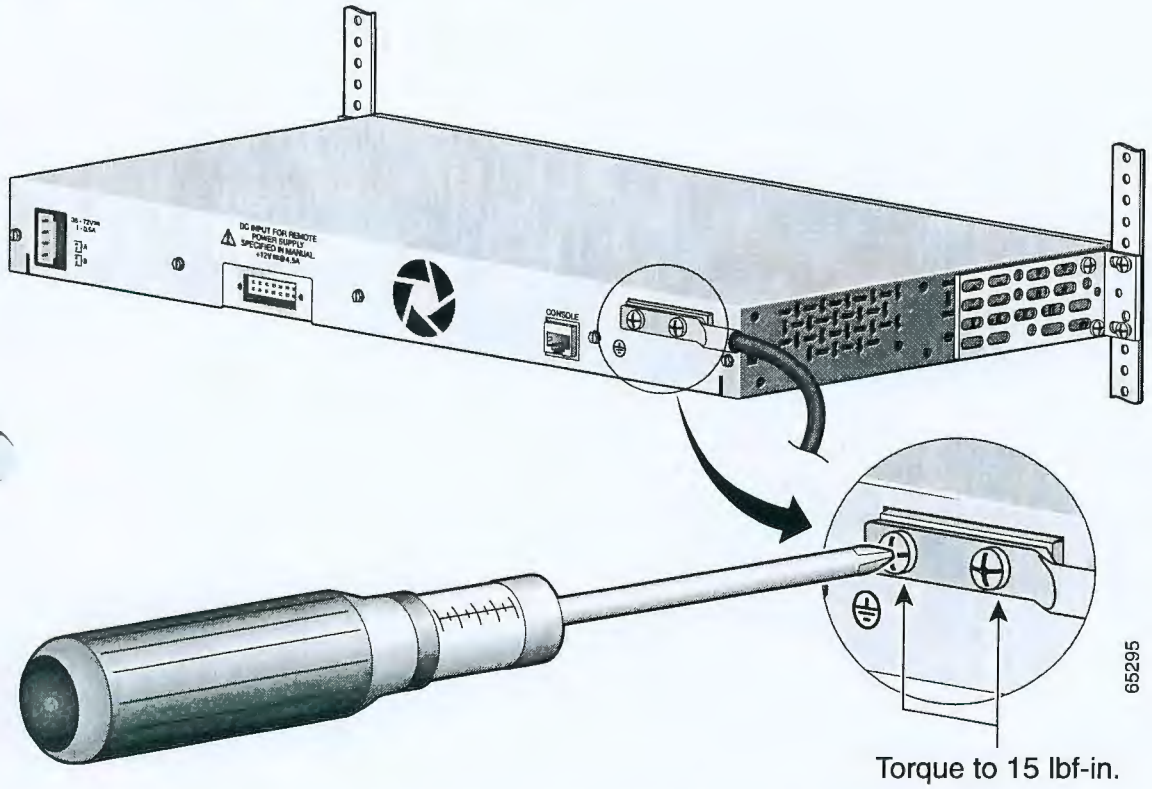


Step 5 Use the two number-10-32 screws to attach the ground lug and wire assembly to the switch rear panel.

Step 6 Using a ratcheting torque screwdriver, torque each ground-lug screw to 15 lbf-in. (240 ounce-force inches [ozf-in.]).

RGS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0973
3690
Doc:

Figure 2-23 Torquing Ground-Lug Screws



Wiring the DC-Input Power Source

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

ECT nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0974
3690
Doc:

Caution You must connect the Catalyst 2950G-24-EI-DC switch only to a DC-input power source that has an input supply voltage from –36 to –72 VDC. If the supply voltage is not in this range, the switch might not operate properly or might be damaged.

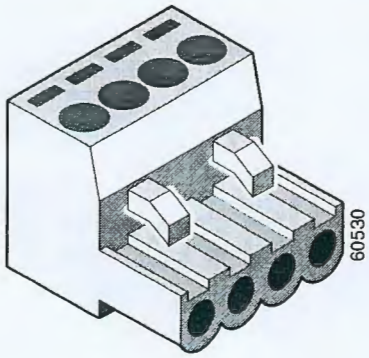
Caution The switch must be installed with 5A-branch-circuit protection.

Note This installation must comply with all applicable codes.

To wire the switch to a DC-input power source, follow these steps:

Step 1 Locate the terminal block plug (see Figure 2-24).

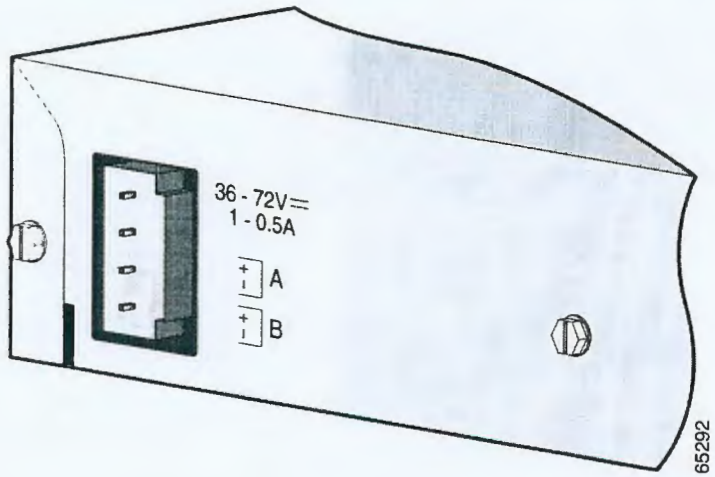
Figure 2-24 Terminal Block Plug



JU.933
A.

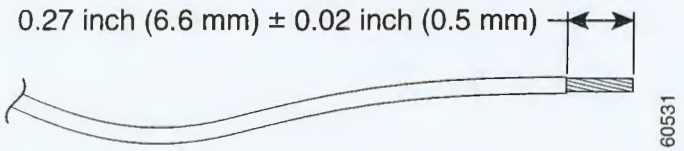
Step 2 Identify the positive and negative feed positions for the terminal block connection. The wiring sequence is positive to positive and negative to negative for both the A and the B feed wires. The switch rear panel identifies the positive and negative positions for both the A and B feed wires.

Figure 2-25 Positive and Negative Positions on the Switch Rear Panel



Step 3 Using an 18-gauge wire-stripping tool, strip each of the four wires coming from the DC-input power source to 0.27 inch (6.6 mm) 0.02 inch (0.5 mm). Do not strip more than 0.29 inch (7.4 mm) of insulation from the wire. Stripping more than the recommended amount of wire can leave exposed wire from the terminal block plug after installation.

Figure 2-26 Stripping the DC-Input Power Source Wire

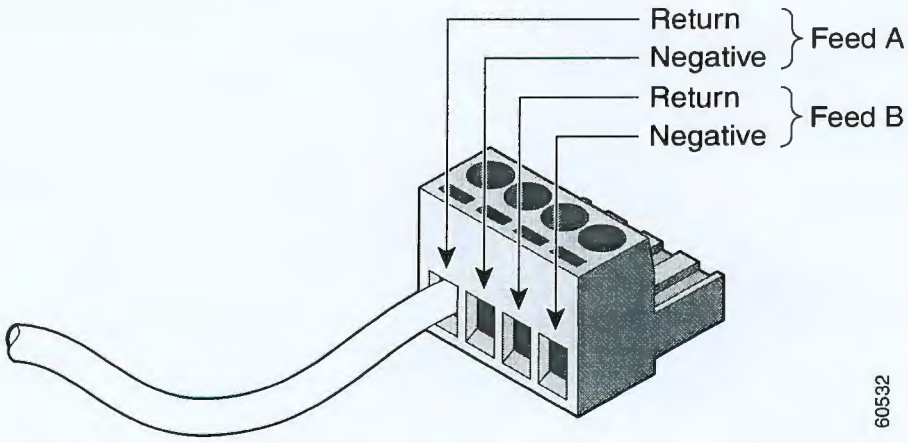


Step 4 Insert the exposed wire of one of the four DC-input power source wires into the terminal block plug, as shown in Figure 2-27. Make sure that you cannot see any wire lead. Only wire *with insulation* should extend from the terminal block.

SQS nº 03/2005 - CN - CPMI - CORREIOS
0976
Fls. Nº
3690
Doc:

Warning **An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.**

Figure 2-27 Inserting Wires in the Terminal Block Plug

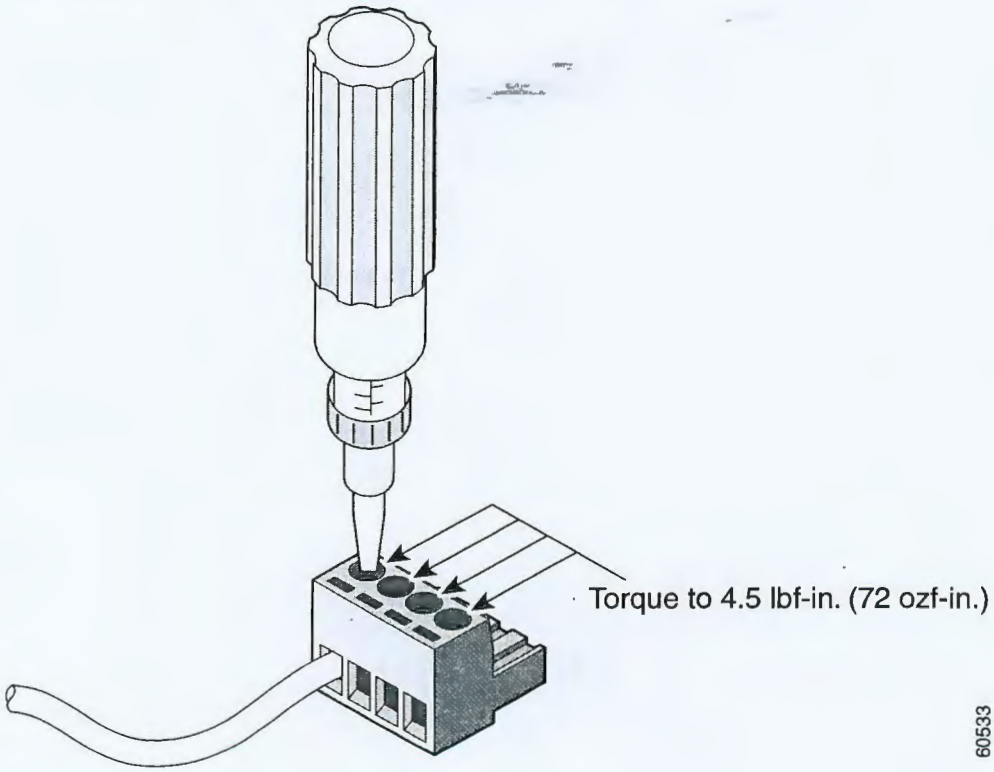


Step 5 Use a ratcheting torque screwdriver to torque the terminal block captive screw (above the installed wire lead) to 4.5 lbf-in. (72 ozf-in.). (See Figure 2-28.)

Caution Do not overtorque the terminal-block captive screws. The recommended maximum torque is 4.5 lbf-in.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0977
3690
Doc:

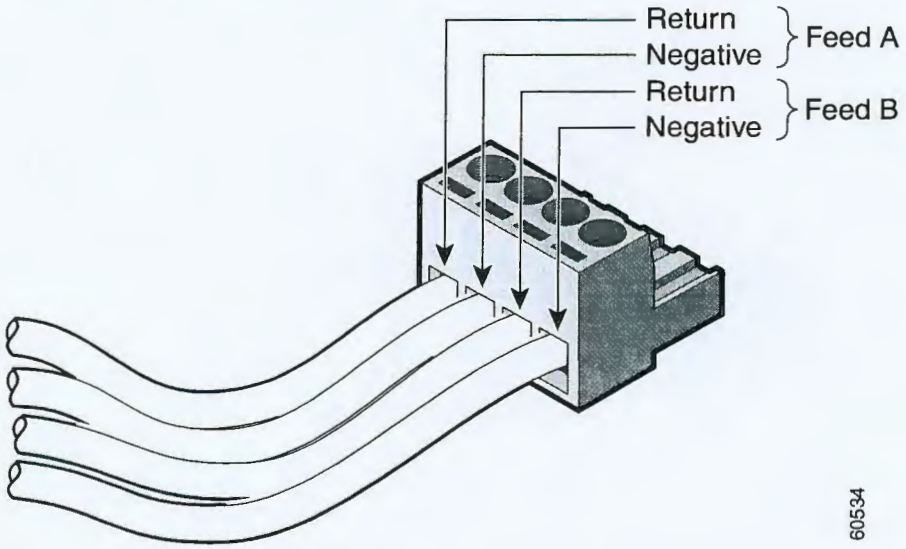
Figure 2-28 Torquing the Terminal-Block Captive Screws



RQS nº 03/2005 - CN - CPML - CORREIOS
Fls. Nº 0978
Doc: 3690

Step 6 Repeat Steps 4 and 5 for the remaining three DC-input power source wires. Figure 2-29 shows the completed wiring of a terminal block plug.

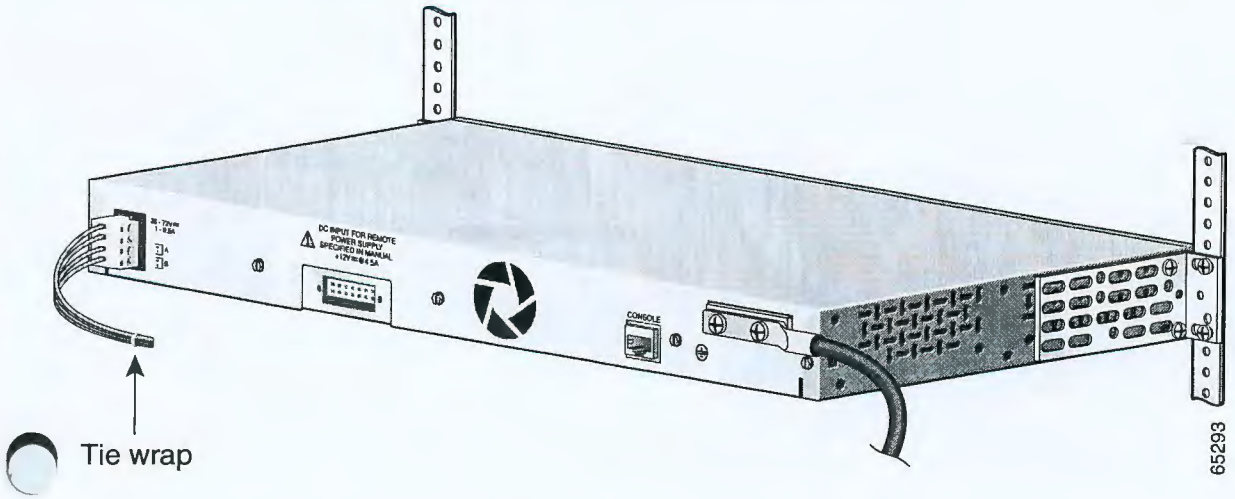
Figure 2-29 Completed Wiring of Terminal Block Plug



Step 7 Insert the terminal block plug in the terminal block header on the switch rear panel (see Figure 2-30).

Caution Secure the wires coming in from the terminal block so that they cannot be disturbed by casual contact. For example, use tie wraps to secure the wires to the rack.

Figure 2-30 Inserting the Terminal Block in the Block Header



Step 8 Remove the tape from the circuit-breaker switch handle, and move the circuit-breaker handle to the on position.

Running POST

After the power is connected, the switch automatically begins POST, a series of tests that verifies that the switch functions properly. When the switch begins POST, the system LED is off. If POST completes successfully, the LED turns green. If POST fails, the LED turns amber. See Chapter 3, "Troubleshooting," to determine a corrective action.

Note POST failures are usually fatal. Call Cisco Systems immediately if your switch does not pass POST.

QS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0980
3690
Doc:

Connecting to 10/100 and 10/100/1000 Ports

The 10/100 ports configure themselves to operate at the speed and duplex settings of attached devices.They operate at 10 or 100 Mbps in half- or full-duplex mode. If the attached devices do not support autonegotiation, you can explicitly set the speed and duplex parameters.

The 10/100/1000 ports configure themselves to operate at the speed setting of attached devices.These ports on Catalyst 2950T-24 switches operate at 10, 100, or 1000 Mbps only in full-duplex mode. If the attached devices do not support autonegotiation, you can explicitly set the speed parameter.

Connecting devices that do not autonegotiate or devices with manually set speed and duplex parameters can reduce performance or result in link failures between the devices. To maximize performance, choose one of these methods for configuring the ports:

- Let the ports autonegotiate both speed and duplex for 10/100 ports and only speed for 10/100/1000 ports.
- Set the speed and duplex parameters on both ends of the connection.

When connecting the ports on the Catalyst 2950G-24-EI-DC switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC switch is suitable only for intrabuilding or nonexposed wiring connections.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 0081
Doc: 3690

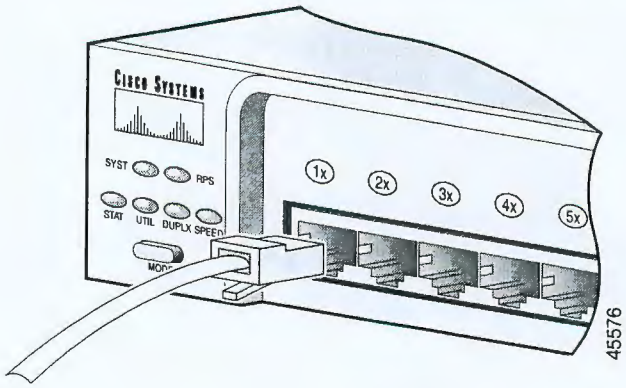
Follow these steps to connect the switch to 10BASE-T, 100BASE-TX, or 1000BASE-T devices:

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a twisted-pair straight-through cable in a front-panel RJ-45 connector, as shown in Figure 2-31, Figure 2-32, and Figure 2-33. When connecting to switches or repeaters, insert a twisted-pair crossover cable. (See the "Cable and Adapter Specifications" section on page B-7 for cable-pinout descriptions.)

Note When connecting to 1000BASE-T devices, be sure to use a four twisted-pair, Category 5 cable.

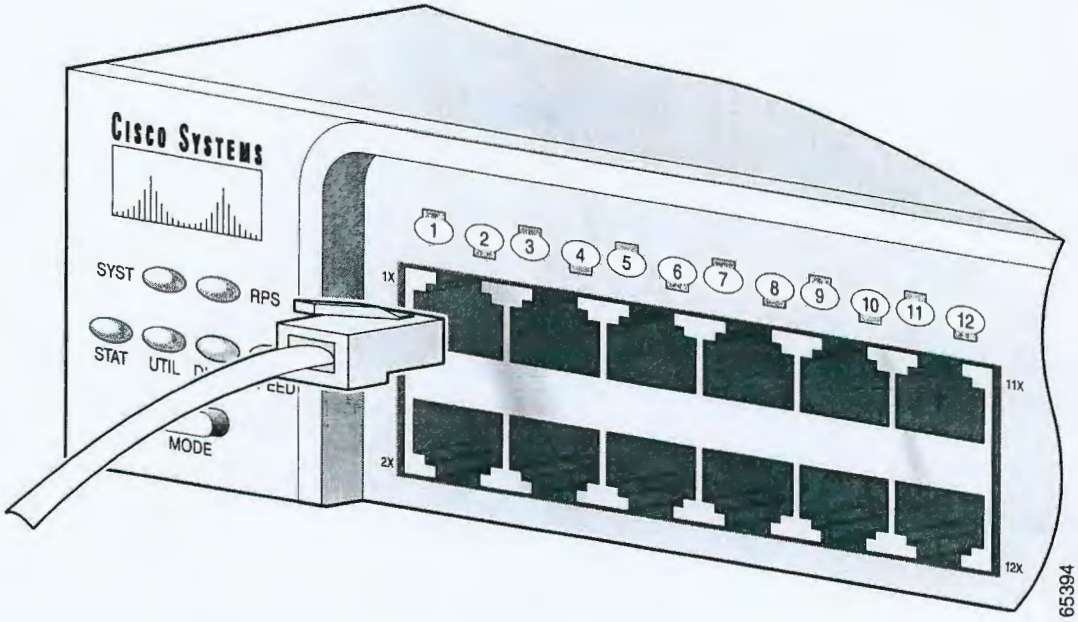
Figure 2-31 Connecting to a Port on Catalyst 2950-12, 2950-24, 2950C-24, 2950SX-24, and 2950T-24 Switches



ROS nº 03/2005 - CN - CPMI – CORREIOS
0983
Fls. Nº
3690
Doc:

14.926
A-

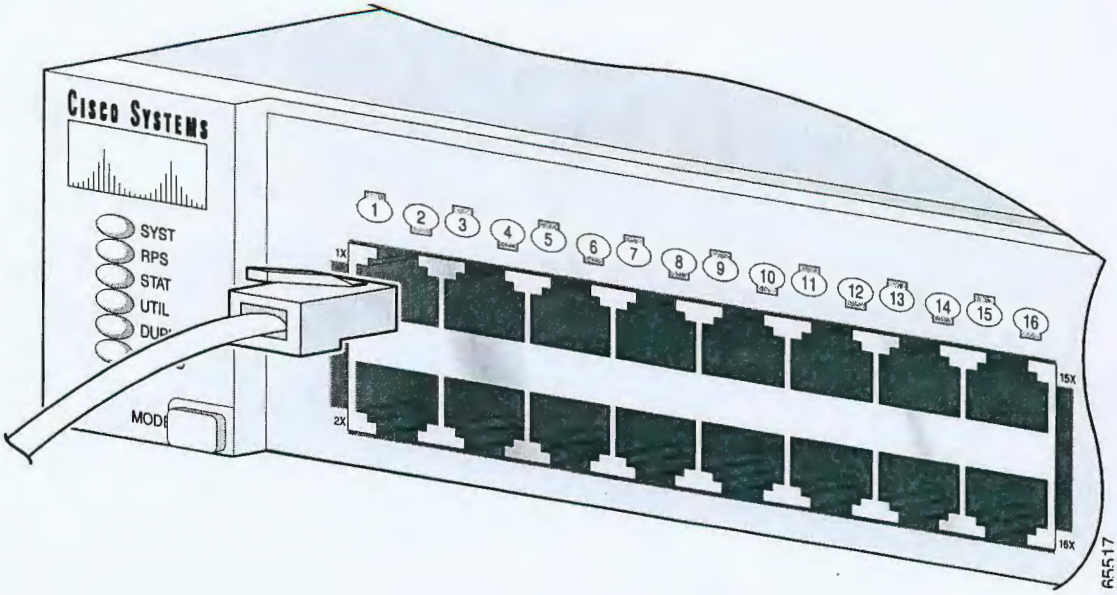
Figure 2-32 Connecting to a Port on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN - CRMI - CORREIOS
Fls. Nº 0983
3690
Doc:

14-925
A.

Figure 2-33 Connecting to a Port on Catalyst 2950G-48-EI Switches



Step 2 Insert the other cable end in an RJ-45 connector on the target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while Spanning Tree Protocol (STP) discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the target device if necessary.

Step 5 Repeat Steps 1 through 4 to connect each port.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0984
Doc: 3690

14.924
A.

Connecting to 100BASE-FX and 1000BASE-SX Ports

The 100BASE-FX and 1000BASE-SX ports operate only in full-duplex mode.

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on another device by using one of the MT-RJ fiber-optic patch cables listed in Table 2-1. Use the Cisco part numbers in Table 2-1 to order the patch cables that you need.

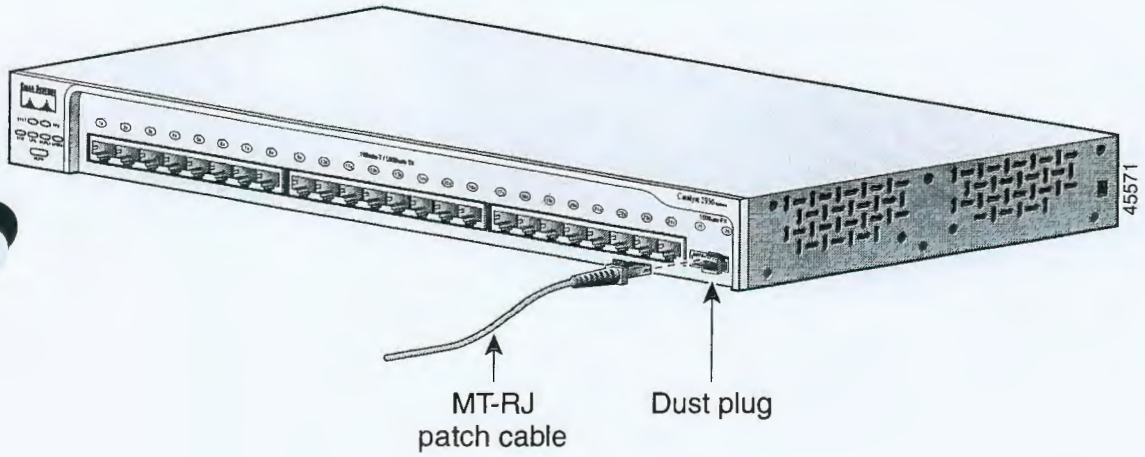
Follow these steps to connect the switch to a 100BASE-FX or 1000BASE-SX device:

Caution Do not remove the dust plugs from the fiber-optic ports or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the fiber-optic ports and cables from contamination and ambient light.

Step 1 Remove the dust plugs from the 100BASE-FX or 1000BASE-SX port and the rubber caps from the MT-RJ patch cable. Store them for future use.

Step 2 Insert the cable in a 100BASE-FX or 1000BASE-SX port. (See Figure 2-34.)

Figure 2-34 Connecting to a 100BASE-FX or 1000BASE-SX Port



ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0985
Doc: 3690

14.923
A.

Step 3 Insert the other cable end in an SC or ST port on the target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the target device if necessary.

Step 6 Repeat Steps 1 through 5 to connect each port.

Connecting to GBIC Module Ports

These sections describe how to connect to a GBIC module port.

- Connecting to 1000BASE-X GBIC Module Ports, page 2-39
- Connecting to 1000BASE-T GBIC Module Ports, page 2-41
- Connecting to GigaStack GBIC Module Ports, page 2-42

For instructions about how to connect to the CWDM GBIC module ports, refer to the documentation that came with that GBIC module.

For detailed instructions about installing, removing, and connecting to the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to the GBIC documentation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0986
Fls. Nº
3690
Doc:

When connecting the ports on the Catalyst 2950G-24-EI-DC switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC switch is suitable only for intrabuilding or nonexposed wiring connections.

Connecting to 1000BASE-X GBIC Module Ports

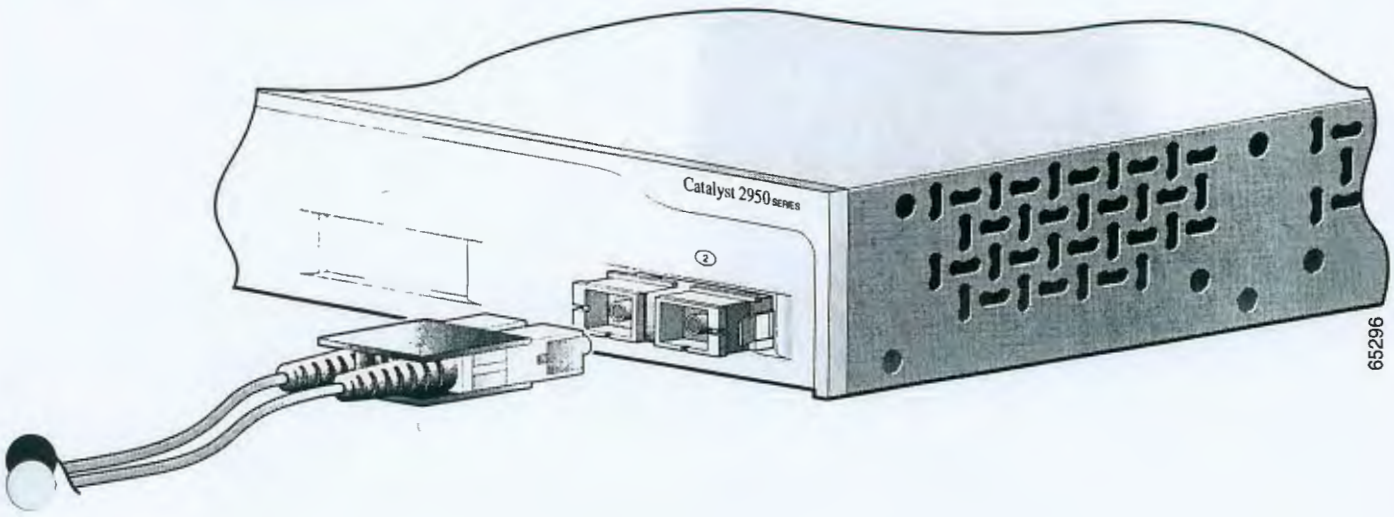
Caution Do not remove the rubber plugs from the GBIC module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the GBIC module ports and cables from contamination and ambient light.

After installing the 1000BASE-X GBIC in the GBIC module slot, follow these steps:

Step 1 Remove the rubber plugs from the GBIC module port, and store them for future use.

Step 2 Insert the SC connector in the fiber-optic receptacle (see Figure 2-35).

Figure 2-35 Connecting to a 1000 BASE-X GBIC Port



Step 3 Insert the other cable end in a fiber-optic receptacle on a target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the switch or target device if necessary.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 3690
Doc:

Connecting to 1000BASE-T GBIC Module Ports

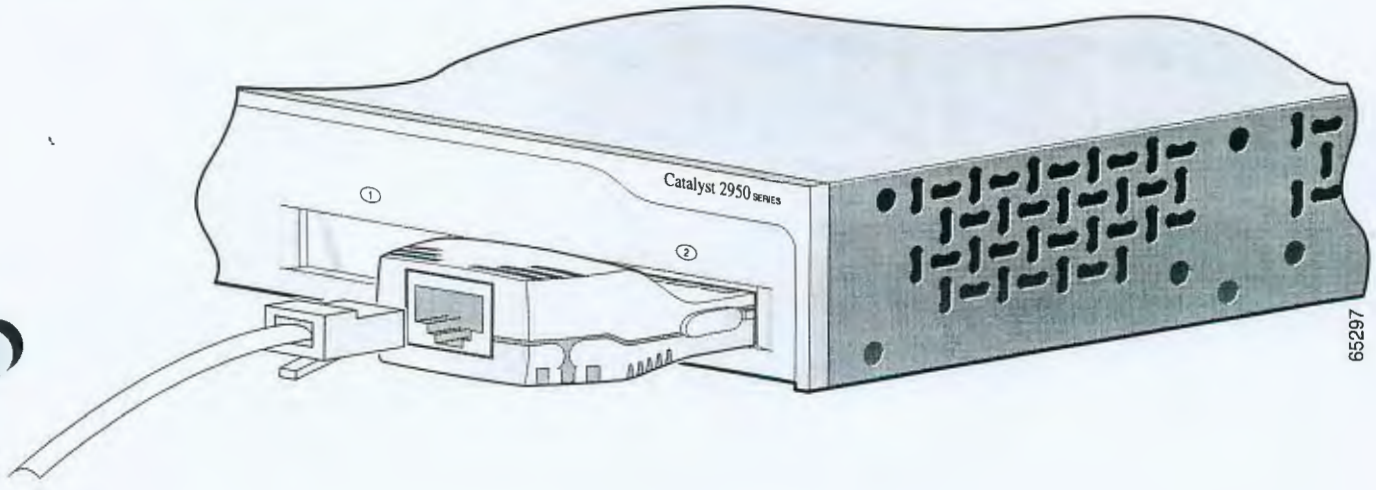
After installing the 1000BASE-T GBIC in the GBIC module slot, follow these steps:

Caution To prevent ESD damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a four twisted-pair, straight-through cable in the RJ-45 connector. When connecting to switches or repeaters, insert a four twisted-pair, crossover cable (see Figure 2-36).

Note When connecting to a 1000BASE-T device, be sure to use a four twisted-pair, Category 5 cable.

Figure 2-36 Connecting to a 1000BASE-T GBIC Port



Step 2 Insert the other cable end in an RJ-45 connector on a target device.

RQS nº 03/2005 - CN - CORREIOS
Fls. Nº 0989
3690
Doc:

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

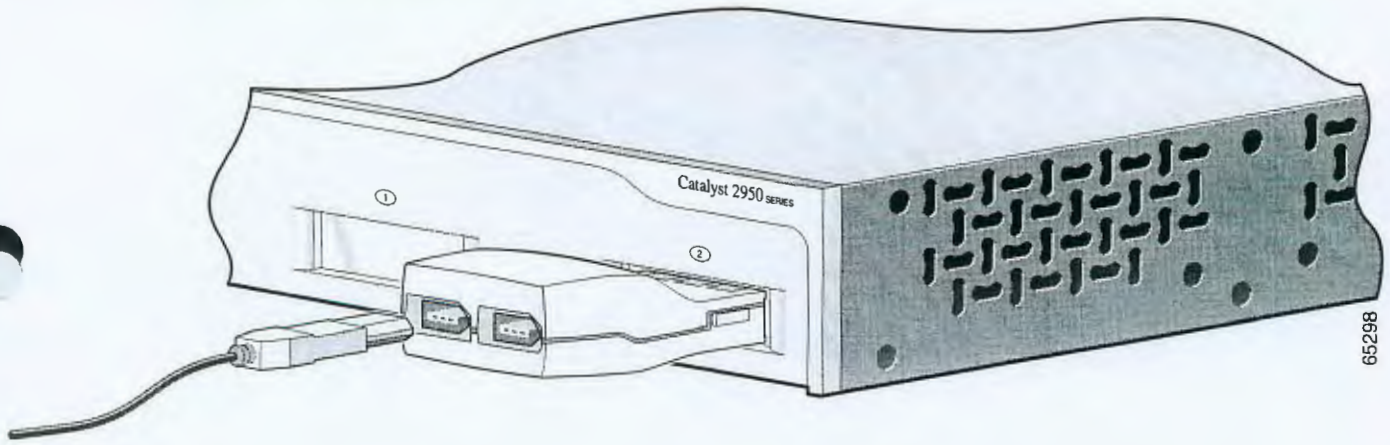
Step 4 Reconfigure and restart the switch or target device, if necessary.

Connecting to GigaStack GBIC Module Ports

After installing the GigaStack GBIC in the GBIC module slot, follow these steps:

Step 1 Insert the GigaStack cable connector in the GBIC (see Figure 2-37).

Figure 2-37 Connecting to a GigaStack GBIC Port



Step 2 Insert the other cable end in a port on a target device.

14.918
A

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the switch or target device, if necessary.

Connecting a PC or a Terminal to the Console Port

If you want to connect a PC to the console port, use the supplied RJ-45-to-DB-9 adapter cable. If you want to connect a terminal to the console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco. For console-port and adapter-pinout information, see the"Cable and Adapter Specifications" section on page B-7.

The PC or terminal must support VT100 terminal emulation. The terminal-emulation software—frequently a PC application such as HyperTerminal or Procomm Plus—makes communication between the switch and your PC or terminal possible during the setup program.

Follow these steps to connect your PC or terminal to the console port:

Step 1 Make sure that your terminal-emulation software is configured to communicate with the switch through hardware flow control.

Step 2 Configure the baud rate and character format of the PC or terminal to match these console-port default characteristics:

- 9600 baud
- Eight data bits
- One stop bit
- No parity

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0991
Doc: 3690

After gaining access to the switch, you can change the port baud rate. Refer to the switch software configuration guide for instructions.

Step 3 Insert the adapter cable in the console port, as shown in Figure 2-38, Figure 2-39, and Figure 2-40. (See the "Cable and Adapter Pinouts" section on page B-10 for pinout descriptions.)

Figure 2-38 Connecting to the Console Port

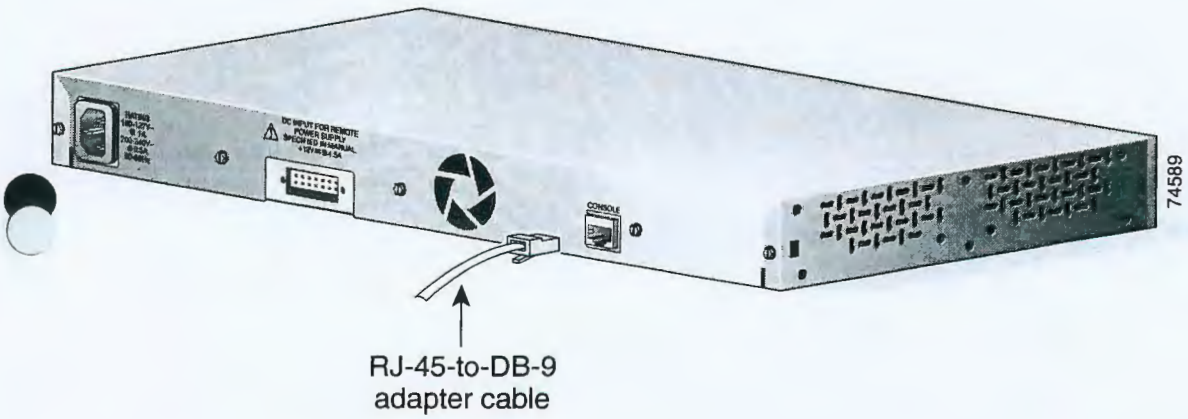
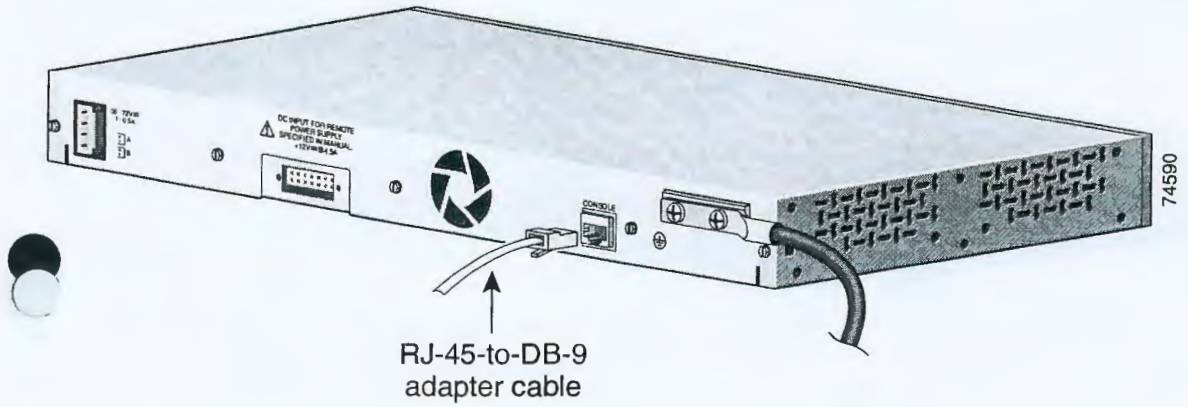
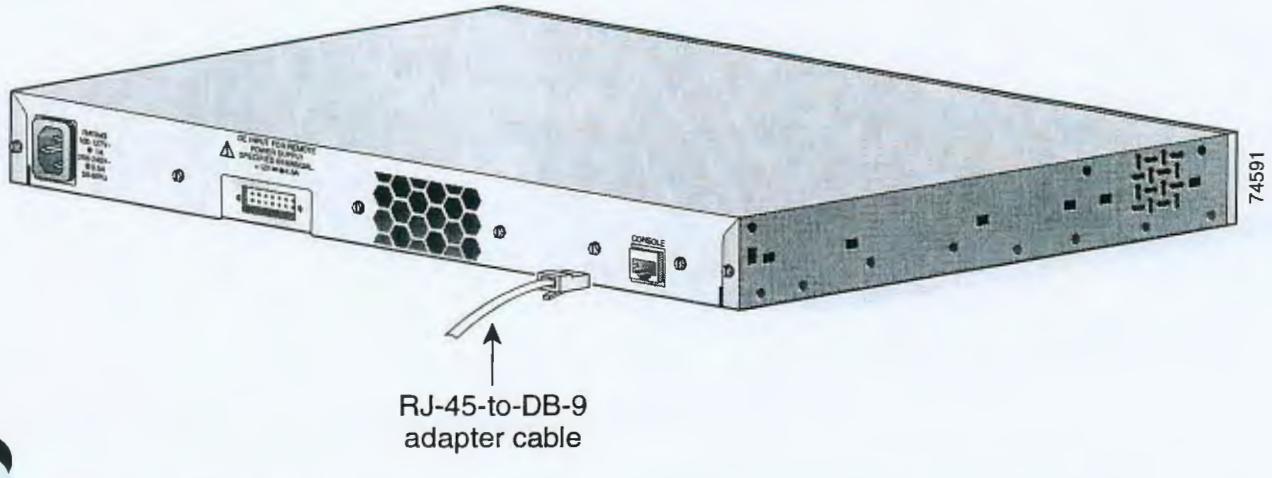


Figure 2-39 Connecting to a Console Port Only on Catalyst 2950G-24-EI-DC Switches



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls 0992
3690

Figure 2-40 Connecting to a Console Port Only on Catalyst 2950G-48-EI Switches



Step 4 Attach the appropriate adapter to the terminal, if needed.

Step 5 Insert the other adapter cable end in the PC or terminal adapter.

Step 6 Start the terminal-emulation software.

Where to Go Next

For information about starting up the switch, refer to the *Release Notes for the Catalyst 2950 Switch.*

For information about configuring the switch, refer to the switch software configuration guide.

RQS nº 03/2005 - CN - CORREIOS
Fls. Nº 0993
Doc: 3690

14-915
A-

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0994
Doc: 3690

14.869
(A-

Switch Tipo 2 doc 7

RQS nº 03.2005 - CN -
CPMI - CORREIOS
FLS Nº 0995
3690

Statement of Direction

1000BASE-T—*Delivering Gigabit Intelligence on Copper Infrastructure*

14.868
A.

AS A MARK OF LEADERSHIP, CISCO IS EXTENDING ITS BREADTH OF GIGABIT PRODUCT SUPPORT TO INCLUDE THE LATEST ETHERNET APPLICATION: 1000BASE-T OR GIGABIT ON COPPER CABLING.

Gigabit Over Copper Cabling

As the leading provider of Gigabit Ethernet and switched internetworking solutions, Cisco Systems is committed to the development of high-performance Ethernet technology and products that provide gigabit-per-second transmission rates to address both service provider and enterprise customer requirements. (See Figure 1, Breadth of Gigabit Ethernet Applications.) As a mark of that leadership, Cisco is extending its breadth of Gigabit product support to include the latest Ethernet application: 1000BASE-T or Gigabit on copper cabling. 1000BASE-T specifies Gigabit Ethernet operation over the Category 5 cabling systems installed according to the specifications of ANSI/TIA/EIA-568A (1995). 1000BASE-T also supports 1000 Mbps operation over the newest emerging EIA/TIA cabling specifications Category 5e.

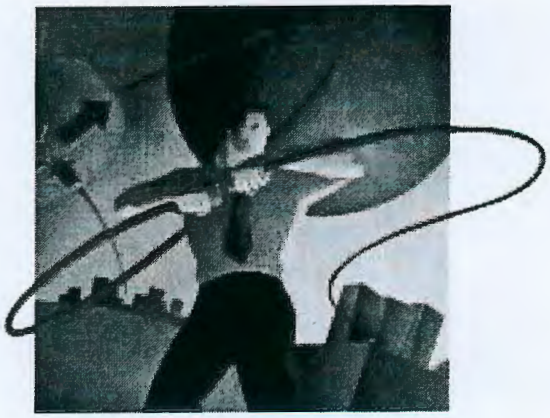
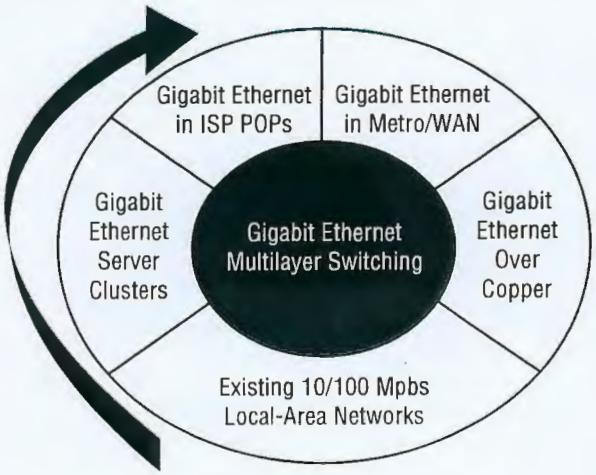


Figure 1 Breadth of Gigabit Ethernet Applications



Cisco will provide not only 1000BASE-T products but also Gigabit Intelligent Network Services for all network managers and planners who require gigabit-per-second speed over Category 5 and Category 5e cabling. More than 80 percent of the cabling inside buildings today is Category 5 copper. By delivering a complete Gigabit on copper networking solution, Cisco enables network managers to scale their wiring closets and data centers to Gigabit speeds while leveraging their investment in installed copper cabling infrastructure.

Gigabit on Copper Applications and Intelligent Network Services

By supporting 1000BASE-T interfaces on its comprehensive product line, Cisco offers enterprise network managers a unique and compelling solution. Because 1000BASE-T is Ethernet, it requires no change to the Ethernet media access control (MAC) or packet format. 1000BASE-T supports all upper- layer services, including all Cisco Intelligent Network Services that operate at Layer 2, Layer 3, and higher of the Open System Interconnection (OSI) seven-layered model: high availability, quality-of-service (QoS), security and policy enforcement, server load balancing (SLB), and Web caching, just to name a few. 1000BASE-T also supports all standard Layer 2 functions such as 802.1p, EtherChannel®, Inter- Switch Link (ISL), virtual local-area network (VLANs), 802.1Q, and spanning tree.

1000BASE-T is the ideal high-speed solution for three application spaces where horizontal copper cabling exists:

- 1000BASE-T uplinks from desktop switches to aggregating switches
- Data centers for server switching
- Wiring closet switches for 10/100/1000 bandwidth to the desktop

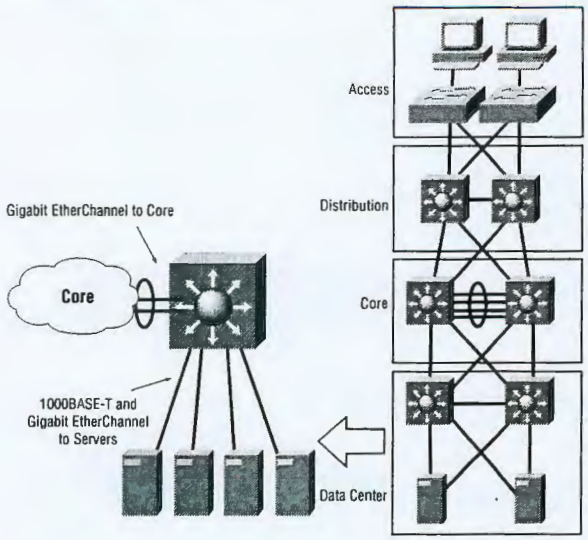
CISCO SYSTEMS

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0996
3690
Doc:

14-867
A-

1000BASE-T in the Data Center

Figure 2 1000BASE-T in the Data Center



When 1000BASE-T NICS become available in volume in mid- and late-CY2000, 1000BASE-T will be used in data centers for server switching and server connectivity as shown in Figure 2. High-performance servers performing such functions as application hosting may be connected to the data-center switch with 1000BASE-T network interface cards (NICs) and Gigabit EtherChannel can be used to create redundant links. Such Gigabit Intelligent Network Services may be applied as:

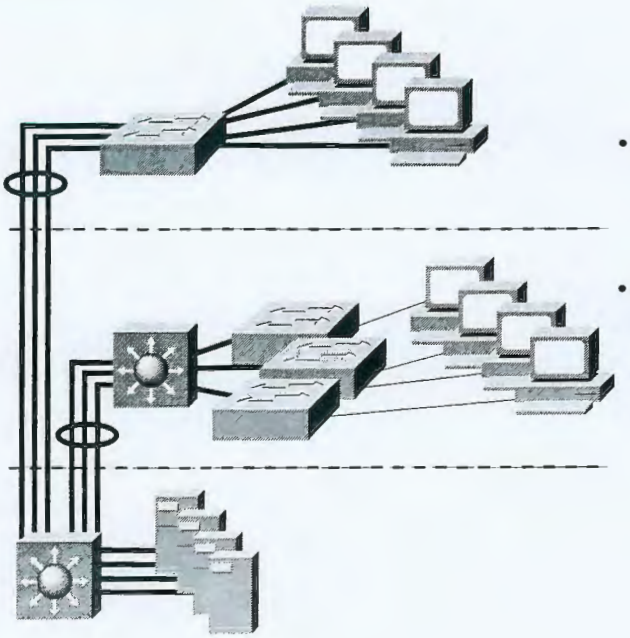
- Server load balancing (SLB)
- Web caching using web caching control protocol (WCCP)
- Packet inspection and classification
- Security features such as intrusion detection and access control lists (ACLs)
- High availability using technologies such as hot standby router protocol (HSRP) and Gigabit EtherChannel (GEC)

1000BASE-T in the Wiring Closet

As 1000BASE-T desktop NICs emerge in early- or mid- CY2001, 1000BASE-T will mature into a high-performance alternative to connect workstations and power desktops to the network (see Figure 3). Figure 4 shows that, in the very near future, high-performance desktops may be attached to the network with 10/100 or 1000BASE-T. Multi-gigabit connectivity to the core of the network may be achieved using Gigabit EtherChannel. For this wiring close application of 1000BASE-T, such Gigabit Intelligent Network Services may be applied as:

- Admission control
- Traffic detection and classification
- QoS/class of service (CoS)
- ACLs

Figure 3 1000BASE-T in Wiring Closets

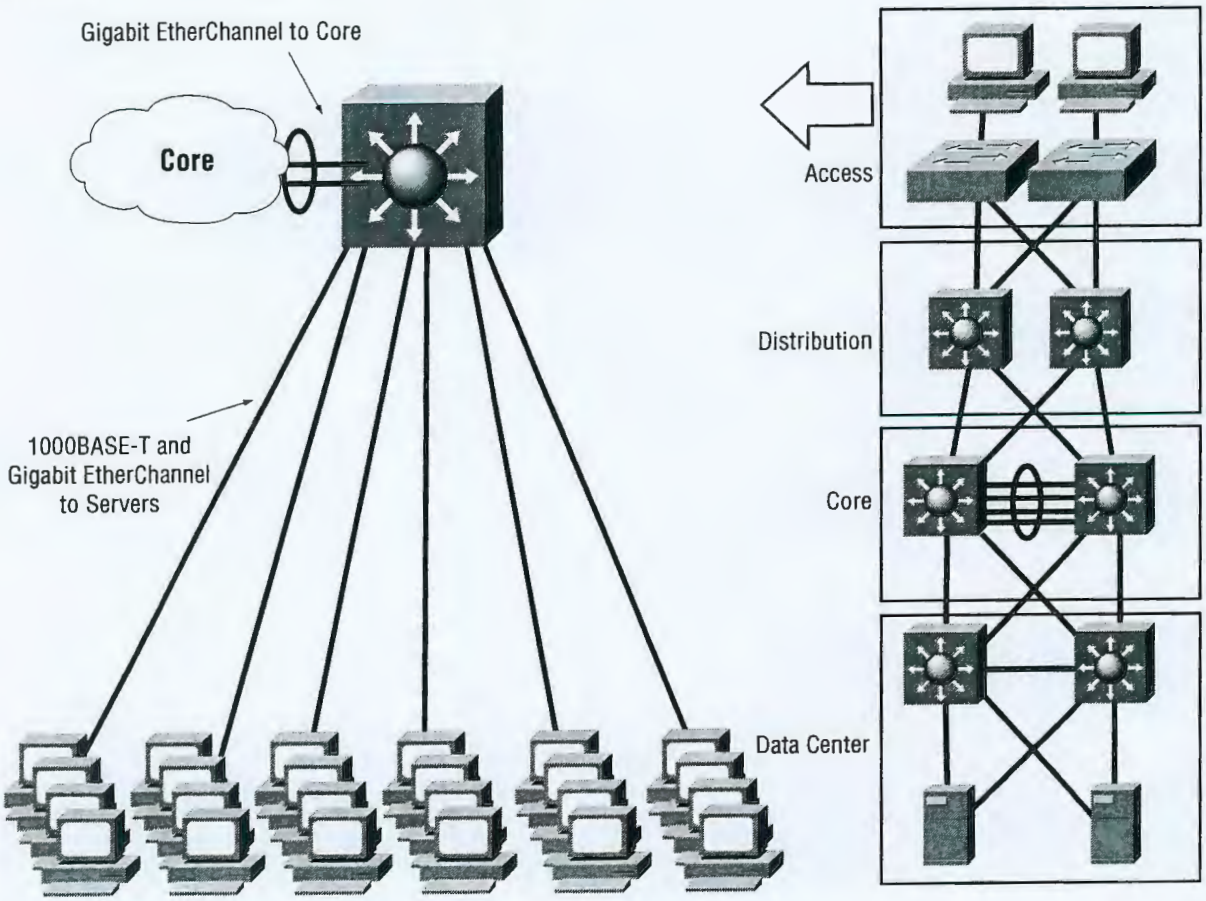


- Desktop Connectivity
  - –To support bandwidth-hungry applications
  - –Cost-effective technology to deliver increased performance to the desktop
- Additional capacity required in the backbone
  - –Use Gigabit EtherChannel to scale Gigabit connections

RQS nº 03/2005 - CN -
CPMI CORREIOS
0997
Fls. Nº
3690
Doc:

14-866
A.

Figure 4 1000BASE-T for Desktop Aggregation

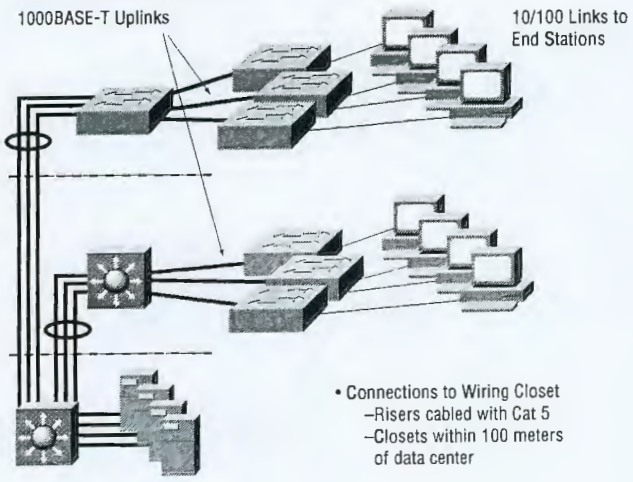


1000BASE-T Uplinks

As Figure 5 shows, one of the first applications for 1000BASE-T will be to serve as an uplink technology offering high-bandwidth connectivity from desktop switches to the next point of aggregation. Often such switch links are deployed over Category 5 cabling with 10/100 Mbps Ethernet desktop connections and a 100BASE-TX uplink. Switches with a slide in uplink module may be upgraded to 1000BASE-T uplinks, giving end stations the opportunity to upgrade from 10 to 100 Mbps links and providing high- bandwidth, gigabit-per-second access to servers and other resources. Gigabit Intelligent Network services may be applied on such links as:

- ACLs
- QoS/CoS
- VLANs

Figure 5 1000BASE-T Uplinks

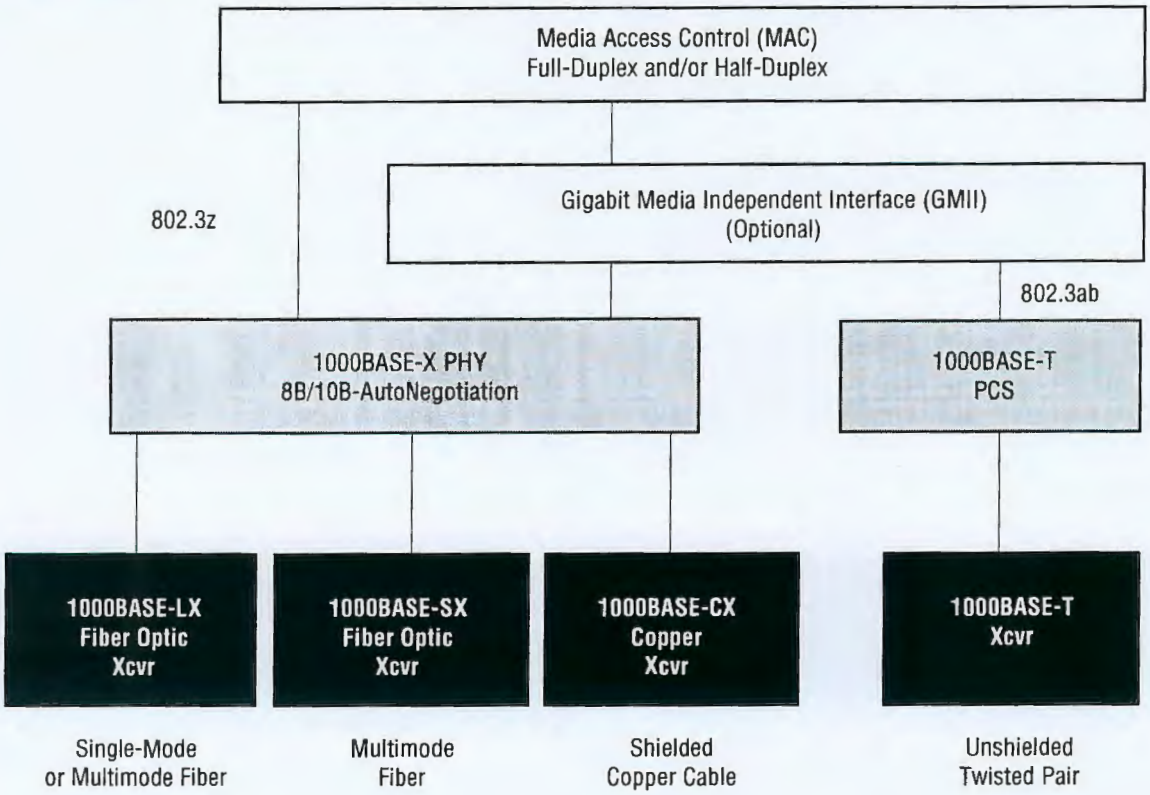


RQS nº 03/2005 - CN -
CPMI - CORREIOS
0998
3690

14.865
A.

1000BASE-T (Gigabit Ethernet over Copper) Technology

Figure 6 GbE Layer Diagram

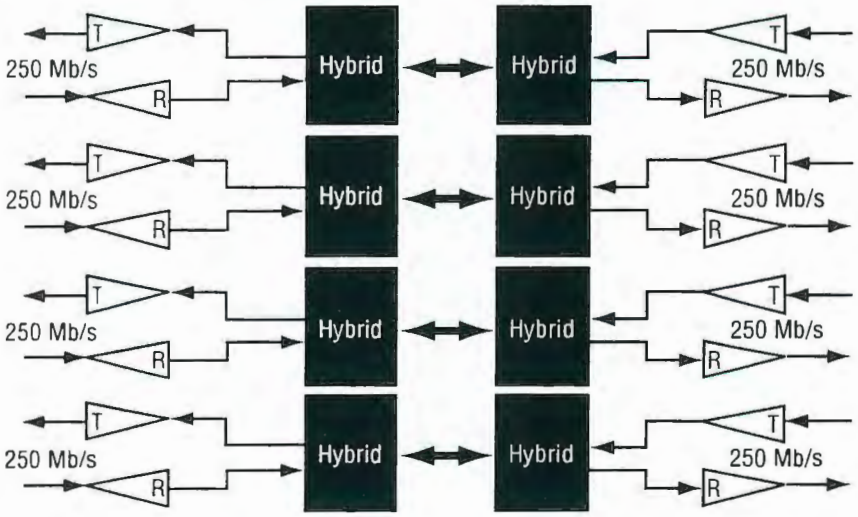


As Figure 6 shows, 1000BASE-T is one of the four physical layers or transceivers defined by the two Gigabit Ethernet standards: IEEE 802.3z or 1000BASE-X and IEEE 802.3ab or 1000BASE-T. 1000BASE-X supports multimode and single- mode fiber media and a short-reach, 25-meter copper jumper. (See Figure 6.) Because most of the cabling installed inside buildings today is Category 5 copper, the IEEE 802.3 1000BASE-T standard supports Gigabit Ethernet operation over the Category 5 cabling systems installed according to the specifications of ANSI/TIA/EIA-568A (1995). As Figure 7 shows, 1000BASE-T works by using all four of the Category 5 pairs to achieve 1000 Mbps operation over the installed Category 5 copper cabling. 1000 Mbps data rates are achieved by sending and receiving a 250 Mbps data stream over each of the four pairs simultaneously (4 X 250 Mbps = 1 Gbps).

RQS nº 03 2003 - CN -
CPMI - CORREIOS
Fls 0999
3690

14.364
A

Figure 7 1000BASE-T: How It Works



In contrast, 100BASE-TX uses two pairs: one to transmit and one to receive. Fast Ethernet on Copper (100BASE-TX) achieves 100 Mbps operation by sending encoded symbols across the link at a symbol rate of 125 Mbaud. A 125 Mbaud symbol rate is required because the 100BASE-TX encoding scheme (called 4B/5B coding) has a bandwidth overhead of 20 percent, the difference between 100 Mbps and 125 Mbaud. Although 1000BASE-T uses a different encoding scheme (five level pulse amplitude modulation or PAM-5), because it maintains the 125 Mbaud symbol rate of 100BASE-TX, 1000BASE-T is backwards compatible with 100BASE-FX at the physical layer. (See Table 1.)

This compatibility feature is significant for network managers and planners because it means that forthcoming generations of 1000BASE-T NICs and switches will support both 100/1000 and 10/100/1000 autonegotiation between Fast Ethernet (100BASE-TX) and Gigabit Ethernet (1000BASE-T). These speed-agile products will enable network managers to deploy 1000BASE-T incrementally into the network. A 100/1000 server NIC may be installed into a new server while the server switch remains 100BASE-TX and vice versa, new 100/1000 server switches may be deployed while maintaining the investment in the existing 100 Mbps server NICs.

Table 1 100BASE-TX, 1000BASE-X, and 1000BASE-T

	100BASE-TX	1000BASE-X	1000BASE-T
Frame format	802.3 Ethernet	802.3 Ethernet	802.3 Ethernet
MAC protocol	802.3 Ethernet	802.3 Ethernet	802.3 Ethernet
Flow control	802.3x	802.3x	802.3x
Symbol rate	125 Mbaud	125 Mbaud	1.25 Gbaud
Data rate	100 Mbps	1000 Mbps	1000 Mbps
Encoding (PCS)	ANSI FDDI 4B/5B	ANSI FC 8B/10B	5 level PAM

Notes:

MAC = media access control protocol

PCS = physical coding sublayer

PAM = pulse amplitude modulation

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. 1000
3690

14.863

The Role of Fiber to the Desktop in the Structured Wiring Paradigm

For standard commercial applications, there is no need to depart from the conventional structured wiring model: fiber in the risers and copper in the horizontal cabling runs. Unless there are security or EMI/RFI concerns about copper cabling or the network manager cannot locate wiring closets 100 meters apart, there is no compelling business reason to deploy fiber to the desktop. Optical transceiver-based switch ports will always be more expensive than copper, and a network manager who runs fiber to the desk will be replacing switch ports three or four times over the life of the cabling plant. Such incremental costs add up over time.

Another reason to avoid running fiber to the desk is that there is currently no way to power network-attached devices from the fiber optic media. In contrast, a LAN phone, IP phones, Web cameras, and other devices may be powered today from the copper cabling. An IEEE 802.3 Task Force is under way to develop standards- based mechanisms to power devices over Category 5 and 5e cabling.

For horizontal runs the standard network application of choice will be 10/100/1000 Ethernet over copper. 1000BASE-T will run on Category 5 and Category 5e cabling at distances to 100 meters. 1000 Mbps at the edge of the network is going to be sufficient bandwidth for almost all customers for the next three to four years.

Looking toward future applications, network managers should note that, while the newer enhanced bandwidth multimode fiber products will support the next Ethernet application, 10 Gigabit Ethernet, enhanced multimode fiber won't support applications beyond 10 Gigabit Ethernet such as 40 Gigabit Ethernet or 100 Gigabit Ethernet. For vertical runs the best choice today is to deploy a hybrid multimode/ single-mode product with the higher bandwidth multimode fiber. By using a hybrid product, network managers achieve backward compatibility with conventional 100BASE-FX, which uses light emitting diodes (LEDs) and will not run on single-mode fiber, and backward compatibility with 1000BASE-SX which is cheaper than 1000BASE-LX. The termination and connectors as well as the optical transceivers (switch ports) for single mode will be more expensive than multimode fiber. For building backbone cabling distances of 300 to 550 meters, single-mode fiber will be the only solution.

1000BASE-T is an important technology for three reasons. First, almost all the cabling installed inside buildings is Category 5. Therefore, 1000BASE-T products enable network planners to deploy Gigabit Ethernet technology over their installed Category 5 cabling plants. Cisco support of the installed horizontal cabling infrastructure with standards- based 1000BASE-T is crucial because, while networking equipment can easily be pulled from a rack, horizontal cabling can be very difficult to replace since it is located inside a wall, ceiling, or raised floor and dispersed across many wiring closets. Second, on a price-per-port basis, 1000BASE-T ports will cost less than 1000BASE-X ports because copper physical sublayers (PHYs) are expected to be less expensive than optical PHYs. Finally, as explained above, 1000BASE-T enables network managers to preserve their investment in existing Ethernet equipment.

Testing the Installed Category 5 Cabling

As stated above, 1000BASE-T specifies Gigabit Ethernet operation over the Category 5 cabling systems installed according to the specifications of ANSI/TIA/EIA-568A (1995). There should be no need to replace existing Category 5 cabling to use 1000BASE-T. The 1000BASE-T standard recommends two additional tests to qualify Category 5 cabling for Gigabit Ethernet operation: return loss and far- end crosstalk (FEXT). Return loss defines the amount of signal energy that is reflected back toward the transmitter due to impedance mismatches in the link (such as those caused by connectors). Far-end crosstalk is noise on a wire pair at the far end from the transmitter (for example, at the receiver) caused by signal leakage from adjoining wire pairs.

These tests are necessary for two reasons. First, Category 5 systems installed prior to the completion of ANSI/TIA/EIA568-A in 1995 may contain connecting hardware that does not comply with the standard. Second, the 1995 cabling standard did not specify these two critical performance parameters. Basic cable testing information is provided by ANSI/TIA/EIA-TSB-67- "Transmission Performance Specifications for Field Testing of Twisted Pair Cabling System." The additional test parameters are published in ANSI/TIA/EIA-TSB 95.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1001
Doc: 3690

14.862
A.

Table 2 Cabling Systems

	Category 5	Category 5e	Category 6 (draft)	Category 7 (draft)
Bandwidth (MHz)	100	100	250	600
Connector type	RJ-45	RJ-45	RJ-45	RJ-45
Standard status	Installation defined in ANSI/TIA/EIA 568A: 1995	In final ballot in TIA committee. Published as Addendum 5 to 568A (TIA/EIA-568-A-5)	In development by TIA TR 42.7.1 and ISO/IEC/SC25/WG3	In development by ISO/IEC/ SC25/WG3
Testing	TIA/EIA TSB 67 TIA/EIA TSB 95 1995 specification does not include tests for return loss and FEXT	Defined in Addendum 5. Specification includes tests for return loss and FEXT	Specification will include tests for return loss and FEXT	Specification will include tests for return loss and FEXT
Comment		Recommended for all new installations	Not a final specification. Products labeled Category 6 may not be in compliance with the final specification	Not a final specification. Expected n ISO/IEC 11801-2000

ISO/IEC11801 and ANSI/TIA/EIA568-A

ISO/IEC118—the International and European cabling standard—is being modified to add return loss and ELFEXT measures to the specifications for Category 5 cabling and will not define a separate Enhanced Category 5 cabling. In contrast, the TIA 41.8.1 Task Force responsible for ANSI/TIA/EIA568-A chose to combine the definitions of current Category 5 cabling practices with the new measures for return loss and far-end crosstalk to create a Category 5e specification. For the installed base of legacy Category 5 cabling, the TIA will specify the measurements for return loss and far-end crosstalk in Technical Service Bulletin ANSI/TIA/EIA-TSB-95.

To sum up, 1000BASE-T specifies Gigabit Ethernet operation over the cabling installed according to the EIA/TIA Category 5 specification. Network managers should check that their installed cabling is indeed compliant with the Category 5 specifications. Also, the 1000BASE-T standard recommends two to qualify the installed Category 5 cable. If a Category 5 cabling plant supports 100BASE-TX operation today to distances of 100 meters, it should support 1000BASE-T to 100 meters.

Category 5e Cabling

As Table 2 shows, the Category 5e cabling standard and the emerging Category 6 specification are supersets of the Category 5 specification. Because the Category 5e specification includes the testing parameters for return loss and far end cross talk, cabling plants certified as Category 5e will support 1000BASE-T operation. Category 5e cabling is recommended for all new installations.

Network managers and planners considering Category 6 installations, should be aware that the specification for Category 6 cabling is not yet formalized. In such cases, network managers should work with their cabling installer to ensure that an installation based on components labeled Category 6 will be upgraded to be compliant with the final Category 6 standard. Because the Category 6 specification will include the testing parameters for return loss and far end cross talk, cabling plants certified as Category 6 will support 1000BASE-T operation.

Conclusions

Cisco is extending its breadth of Gigabit product support to include the latest Ethernet application: 1000BASE-T or Gigabit on copper cabling. 1000BASE-T specifies Gigabit Ethernet operation over the Category 5 cabling systems installed according to the specifications of ANSI/TIA/EIA-568A (1995). 1000BASE-T also supports 1000 Mbps operation over the newest EIA/TIA cabling specification Category 5e. Because 1000BASE-T is Ethernet, it requires no change to the Ethernet MAC or packet format. 1000BASE-T therefore supports all upper-layer services, including all Cisco Intelligent Network Services that operate at Layer 2, Layer 3, and higher of the OSI seven-layered model. 1000BASE-T also supports all standard Layer 2 functions: 802.1p, 802.1Q, Gigabit Ethernet- Channel, Fast EtherChannel, ISL, VLANs, and spanning tree. The primary initial applications for 1000BASE-T will be switch uplinks and data-center switching. As 1000BASE-T desktop NICs emerge, 1000BASE-T will eventually extend to the desktop for workstations demanding the highest-speed connections to the network.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
FI 1002
3690

Web References

www.gigabit-ethernet.org

www.bicsi.com

http://www.mohawk-cdt.com/main-n.html

14.861
A.

Glossary

- **Echo**—See return loss.
- **FEXT**—Far-end crosstalk is noise on a wire pair at the far end from the transmitter (for example, at the receiver) caused by signal leakage from adjoining wire pairs
- **MAC**—Media access control protocol which manages access to the physical media
- **PAM**—Pulse amplitude modulation
- **PCS**—Physical coding sublayer. Codes such as 8B/10B or 4B/10B are used to transmit data into forms suitable for the physical media and decoding it at the receiver
- **Return loss**—Echo or return loss defines the amount of signal energy that is reflected back toward the transmitter due to impedance mismatches in the link (such as those caused by connectors

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at http://www.cisco.com/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000 Cisco Systems, Inc. All rights reserved. Printed in the USA. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other resellers. (9912R)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1003
Doc: 3890

14.860
A.

Switch Tipo 5 doc1

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1004
Doc: 3690

Cisco Systems

Data Sheet

Cisco **VPN 3000** Series Concentrator

Introduction

The Cisco® VPN Series 3000 Concentrator allow corporations to take full advantage of the unprecedented cost savings, flexibility, performance, and reliability of remote access VPN connections. Corporations use VPNs to establish secure, end-to-end private network connections over a public networking infrastructure. VPNs have become the logical solution for remote-access connectivity for two main reasons:

- Deploying a remote-access VPN enables corporations to reduce communications expenses by using the local dialup infrastructures of Internet service providers.
- Remote Access VPNs allow mobile workers, telecommuters and day extenders to take advantage of broadband connectivity.

To fully realize the benefits of high-performance, remote-access VPNs, a corporation must deploy a robust, highly available VPN solution, and dedicated VPN devices are optimal for this purpose.

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution for enterprise-class deployment. A standards-based, asy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote access VPNs. Incorporating the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications.

Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP/SEP-E) modules, enable users to easily add capacity and throughput.

The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, the Microsoft Windows 2000/XP L2TP/IPsec Client, the Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium (ME), Windows NT Workstation 4.0, and Microsoft PPTP.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1005
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.858
A

Five Models

The Cisco VPN 3000 Concentrator is available in five different models:

Cisco VPN 3005 Concentrator

The Cisco VPN 3005 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Encryption processing is performed in software. The Cisco VPN 3005 does not have built-in upgrade capability.

Cisco VPN 3015 Concentrator

The Cisco VPN 3015 Concentrator is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous sessions. Like the Cisco VPN 3005, encryption processing is performed in software, but the Cisco VPN 3015 is also field-upgradable to the Cisco VPN 3030 and 3060 models.

Cisco VPN 3030 Concentrator

The Cisco VPN 3030 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3(50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 is field-upgradeable to the Cisco VPN 3060. Redundant and nonredundant configurations are available.

Cisco VPN 3060 Concentrator

The Cisco VPN 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and nonredundant configurations are available.

Cisco VPN 3080 Concentrator

The Cisco VPN 3080 Concentrator is optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous remote access sessions. Specialized SEP modules perform hardware-based acceleration. The VPN 3080 is available in a fully redundant configuration only.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1006
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14-857
A

Models Comparison

Table 1 The Cisco VPN 3000 Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous Users[1]	100	100	1,500	5,000	10,000
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Available Expansion Slots	0	4	3	2	2
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	–	–	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

1. For planning purposes, a simultaneous user is considered to be a remote access VPN user connected in all tunneling mode—this includes one IKE Security Association and two unidirectional IPsec SAs (Security Associations). For environments with rekeying or split tunneling, we recommend using a VPN remote access load-balancing environment with spare capacity because these particular sessions will use additional system resources that otherwise would be used to support additional users. The Cisco VPN 3000 Series Concentrator supports the entire range of enterprise applications.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator. This thin design, IPsec-compliant implementation is provided with the Cisco VPN 3000 Concentrator and is licensed for an unlimited number of users. The client can be pre-configured for mass deployments and the initial logons require very little user intervention. VPN access policies are created and stored centrally in the Cisco VPN 3000 Concentrator and pushed to the client when a connection is established.

RQS nº 03/2005 - CN - CPM 1007 CORREIOS
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14856
A.

Features and Benefits

Product Highlights

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (Cisco VPN 3030–3080).
- Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPsec connections.

Scalability (Cisco VPN 3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
- System architecture is designed to supply consistent, high-availability performance.
- All digital design provides the highest reliability and 24-hour continuous operation.
- Robust instrumentation package provides run-time monitoring and alerts.
- Microsoft compatibility offers large-scale client deployment and smooth integration with related systems.

Security

- Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.
- Firewall capabilities through stateless packet filtering and address translation to ensure the required security of a corporate LAN.
- User and group level management offers maximum flexibility.

High Availability

- Redundant subsystems and multichassis failover capabilities ensure maximum system uptime.
- Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, SSHv1, and using a console port. Files can be accessed through HTTPS, FTP, and SSH Copy (SCP).
- Configuration and monitoring capability is provided for both the enterprise and the service provider.
- Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies. For larger scale deployments, the VPN 3000 Concentrators are supported in several Cisco network management applications. Those applications include:
  - *IP Solution Center (ISC)*—Provisions site-to-site and remote access VPN services
  - *VPN Monitor*—Monitors and reports on remote access and site-to-site VPN tunnel connections
  - *Resource Manager Essentials (RME)*—Provides operational management features such as software distribution, syslog reporting, inventory management
  - *CiscoView*—Provides real time system status monitoring

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1008
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14-855
A.

Technical Specifications

Hardware

Processor

- Motorola PowerPC Processor

Memory

- Redundant system images (Flash)
- Variable memory options (see chart)

Encryption

- *Cisco VPN 3005, 3015*—Software encryption
- *Cisco VPN 3030–3080*—Hardware encryption

Embedded LAN Interfaces

- *Cisco VPN 3005*—Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted)
- *Cisco VPN 3015–3080*—Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted and DMZ)

Instrumentation

- *Cisco VPN 3005 Front panel*—Unit status indicator
- *Cisco VPN 3005 Rear panel*—Status LEDs for Ethernet ports
- *Cisco VPN 3015-3080 Front panel*—Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan
- *Cisco VPN 3015–3080 Rear panel*—Status LEDs for Ethernet modules, expansion modules, power supplies
- *Cisco VPN 3015–3080*—Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Software

Client Software Compatibility

- Cisco VPN Client (IPsec) for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit), and Mac OS X 10.2 (Jaguar), including centralized split-tunneling control and data compression
- Microsoft PPTP/MPPE/MPPC, MSCHAPv1/v2, EAP/ RADIUS pass-through for EAP/TLS and EAP/GTC support
- Microsoft L2TP/IPsec forWindows 2000/XP (including XP DHCP option for route population)
- Microsoft L2TP/IPsec for Windows 98, Windows Millennium (ME), and Windows NT Workstation 4.0
- MovianVPN (Certicom) Handheld VPN Client with ECC
- Netlock (Mac OS 8 & 9) VPN Client

Tunneling Protocols

- IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with auto-detection and fragmentation avoidance), IPsec/TCP
- Support for Easy VPN (client and network extension mode)

RGS nº 03/2005 - CN - CPMI - CORREIOS
1009
Fls. Nº
3690
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14-854
A.

Encryption/Authentication

- IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128, 192, 256-bit) with MD5 or SHA, MPPE using 40/128-bit RC4

Key Management

- Internet Key Exchange (IKE)
- Diffie-Hellman (DH) Groups 1, 2, 5, 7 (ECDH)

Routing

- RIP, RIP2, OSPF, RRI (Reverse Route Injection), static, automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
- IPsec fragmentation policiy control, including support for Path MTU Discovery (PMTUD)
- Interface MTU control

Third-Party Compatibility

- Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Macintosh and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, SA Keon

High Availability

- VRRP protocol for multi-chassis redundancy and fail-over
- Remote Access Load Balancing clusters
- Destination pooling for client-based fail-over and connection re-establishment
- Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015–3080)

Management

Configuration

- Embedded management interface is accessible through console port, Telnet, SSHv1, and Secure HTTP (HTTPS)
- Administrator access is configurable for five levels of authorization. Authentication can be performed externally through TACACS+
- Role-based management policy separates functions for service provider and end-user management

Monitoring

- Event logging and notification through e-mail (SMTP)
- Automatic FTP backup of event logs
- SNMP MIB-II support
- Configurable SNMP traps
- Syslog output
- System status
- Session data (including client assign IP, encryption type connection duration, client OS, version, etc)
- General statistics

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1010
3690
Doc:

1453
A.

Security

Authentication and Accounting Servers

- Support for redundant external authentication servers:
  - RADIUS
  - Kerberos/Active Directory authentication
  - Microsoft NT Domain authentication
  - Microsoft NT Domain authentication with Password Expiration (MSCHAPv2)

RSA Security Dynamics (SecurID Ready), including native support for RSA 5 (Load Balancing, Resiliency)

- User authorization through LDAP or RADIUS
- Internal Authentication server for up to 100 users
- X.509v3 digital certificates (including CRL/LDAP and CRL/HTTP, CRL Caching and Backup CRL Distribution Point support)
- RADIUS accounting
- TACACS+ Administrative user authentication

Internet-Based Packet Filtering

- Source and destination IP address
- Port and protocol type
- Fragment protection
- FTP session filtering
- Site-to-Site Filters and NAT (for overlapping address space)

Policy Management

- By individual user or group
  - Filter profiles (defined internally or externally)
  - Idle and maximum session timeouts
  - Time and day access control
  - Tunneling protocol and security authorization profiles
  - IP Pool
  - Authentication Servers

Certification

- FIPS 140-2 Level 2 (3.6) in process, FIPS 140-1 Level 2 (3.1), VPNC

Ports

- Console port-Asynchronous serial (DB-9)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Physical Characteristics

Concentrator	Cisco VPN 3005	CiscoVPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Height	1.75" (4.45cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)
Width	17.5" (44.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)
Depth	11.5" (29.21cm)	–	–	–	–
Unit without front bezel or SEPS/PS	–	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)
Unit with front bezel, no SEPS/PS	–	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)
Unit with front bezel and SEPS/PS	–	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)
Weight	8.5 lbs(3.9kg)	27 lbs(12.3kg)	28 lbs(12.7kg)	33 lbs(15kg)	33 lbs(15kg)

Table 3 Power Type and Requirements

Concentrator	Cisco VPN 3005	CiscoVPN 3015-3080
Nominal	15 watts (51.22BTU/hr)	35 watts (119.50BTU/hr)
Maximum	25 watts (85.36BTU/hr)	50 watts (170.72BTU/hr)
Input Voltage	100-240VAC	100-240VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

Environmental

- Temperature: 32 to 131 F (0 to 55 C) operating; –4 to 176 F (–40 to 70 C) nonoperating
- Humidity: 0 to 95 percent noncondensing

Regulatory Compliance

- CE Marking

Safety

- UL 1950, CSA

EMC

- FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN50082-1, AS/NZS 3548 Class A, VCCI Class A

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1012
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.851
A.

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

03/2005 - CN
CPMI - CORREIOS
Fls. 4013
Doc. 3690

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW4512 0403

14-850
VA.

Switch Tipo 5 doc 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 1014
Doc. 3690

14.849

Data Sheet

Cisco Secure **Access Control Server** Version 3.2 for Windows

The Cisco® Secure Access Control Server (ACS) provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure.

Introduction

With the ever-increasing methods of accessing networks today, security breaches and uncontrolled user access are becoming a primary concern. With the increased usage of the Internet, network administrators are challenged to identify devices as well as users, to guarantee secure transactions, and to prevent the spread of viruses and denial-of-service (DoS) attacks. These challenges exist not only at the perimeter but also inside a network. The wide adoption of 802.11 wireless LAN and the high-speed, always-on Internet connections (such as DSL and cable) are only making these challenges more severe from within an organization's network. Investing in identity networking technologies that can mitigate these ubiquitous security vulnerabilities is worth considering from both an operational and a return-on-investment perspective.

These changing network dynamics and increased security threats have driven new opportunities in access control management solutions. According to the latest report by IDC, security authentication, authorization, and accounting (AAA) solutions represent the fastest growing segment in the security software market, with a 22-percent compound annual growth rate (CAGR) throughout 2006. As AAA becomes more available throughout the network and the requirement to control user access expands beyond simple dialup, new trends (including expanded authentication, tracking, and audit management) are emerging that require identity-networking solutions to be pervasive, scalable, and relevant throughout the network. In particular, identity networking solutions must address user access from an expanding set of network access points (that is, voice, video, virtual private network [VPN], firewalls, content, storage, wireless, DSL, and cable).

Stronger forms of authentication, such as public key infrastructure (PKI) and two-factor authentication, are now being used to control users accessing corporate resources from public networks and VPN. Network administrators are looking for solutions that provide flexible authorization policies that are tied not only to who the user is at the end point, but also to the service type that the user has access to. Lastly, the ability to track and monitor the behavior of network users, in a manner independent from the access medium through which users choose to connect, is of primary importance in isolating unwanted and excessive use of valuable network resources.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1015
Doc. 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.843
A.

Identity networking and the ability to provision the network to user- or device-specific services are now possible with the Cisco Secure ACS. The Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS server or TACACS+ server. The Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking solution, thereby allowing for greater flexibility and mobility, increased security, and user productivity gains. The Cisco Secure ACS greatly reduces the administrative and management burden involved in scaling user and network administrative access to your network. By using a central database for all user accounts, the Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network. As an accounting service, the Cisco Secure ACS reduces IT operating costs by providing detailed reporting and monitoring capabilities of network users' behavior and by keeping a record of every access connection and device configuration change across the entire network.

The Cisco Secure ACS provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security-management applications. The Cisco Secure ACS ensures enforcement of assigned policies by allowing network administrators to control:

- Who can log in to the network
- What privileges each user has in the network
- What accounting information is recorded in terms of security audits or account billing
- What access and command controls are enabled for each configuration administrator

The Cisco Secure ACS supports a wide array of access connection types, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP (VoIP), firewalls, and VPNs.

The Cisco Secure ACS is a key component of the Cisco Identity-Based Networking Services (IBNS) architecture. Cisco IBNS is based on port security standards such as 802.1X (IEEE standard for port-based network access control) and Extensible Authentication Protocol (EAP) to extend security AAA inside the LAN when, historically, access control was managed at the perimeter of the network. New policy controls (such as per-user quotas and virtual LANs [VLANs]) are possible with this new architecture, now that the authenticator (switch or wireless access point) becomes a RADIUS client capable of querying an AAA server for these controls. Cisco IBNS offers greater flexibility and mobility to stratified users by combining access control and user profiles. This combination enhances secure network connectivity, services, and applications, allowing enterprises to increase user productivity and reduce operating costs. Cisco IBNS, combined with the Cisco Secure ACS, allows the network administrator to implement true, identity-based network access control and policy enforcement at the user and port levels. It provides user and device identification with policies that are centrally created and administered by the Cisco Secure ACS while using secure and reliable strong authentication technologies (such as one-time-token or smartcard authentication methods).

In addition to offering dynamic, port-based authentication for securing network access based on an identity, the Cisco IBNS architecture, in conjunction with the Cisco Secure ACS, offers the following additional per-user or per-device policy assignments:

- Time-of-day and day-of-week restrictions
- Network access server IP filter that restricts user and switch access based on network-access-server IP address
- Media Access Control (MAC) address filtering that restricts authentication of devices based on their MAC addresses
- Per-user VLANs
- Per-user ACLs

CPMI - CORREIOS
Fls. 1016
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Up to version 3.1, Cisco Secure ACS has been available as software for Windows installations. Version 3.2 introduces a new, secure, appliance-based offering for Cisco Secure ACS. The Cisco Secure ACS Solution Engine, a 1-rack-unit (1-RU) security-hardened appliance with a preinstalled Cisco Secure ACS license, provides essentially the same features and functions as the Cisco Secure ACS for Windows, in a dedicated, application-specific appliance package.

The Cisco Secure ACS Solution Engine provides a zero-touch installation and highly reliable AAA solution with increased total-cost-of-ownership protection through high availability and simplified day-to-day operation of the Cisco Secure ACS service. The Cisco Secure ACS Solution Engine also includes additional features specific to its operation and management. For more information, refer to the Cisco Secure ACS Solution Engine data sheet.

Cisco Secure ACS 3.2 adds new Extensible Authentication Protocol (EAP) enhancements to support Protected EAP (PEAP) for Microsoft Windows clients. PEAP retains the security benefits of Cisco EAP wireless (LEAP) while providing more extensibility and support for one-time-token authentication. PEAP is a draft in the Internet Engineering Task Force (IETF) Internet Standards group. Cisco Secure ACS Version 3.2 adds support for machine authentication (using EAP-Transport Layer Security [TLS] or PEAP) on secure 802.1X ports, further extending the Cisco IBNS scope. This capability is crucial for device control access in an 802.1X secure environment where port access is blocked until a user has successfully been identified behind an 802.1X-provisioned port. Also new to Cisco Secure ACS 3.2 are EAP-TLS enhancements that provide expanded PKI authentication into open-database-connectivity (ODBC) databases and improved EAP-TLS domain search capabilities.

Features and Benefits

New Features for Cisco Secure ACS Version 3.2

- *PEAP support for Microsoft Windows clients*—Cisco Secure ACS 3.2 adds support for Microsoft PEAP supplicants available today for Windows 98, NT, 2000, and XP. The Microsoft PEAP supplicant supports client authentication only by MS-CHAPv2, as compared to Cisco PEAP supplicant (available through Cisco Aironet® wireless adapters), which supports client authentication by logon passwords or one-time passwords. Unlike the Microsoft PEAP supplicant the Cisco PEAP supplicant provides support for one-time-token authentication and powerful extensibility of non-MSCHAP end-user databases such as Lightweight Directory Access Protocol (LDAP), Novell Directory Service (NDS), and ODBC. Cisco Secure ACS 3.2 allows selection of Microsoft PEAP or Cisco PEAP from its EAP configuration page.
- *LDAP multithreading*—Cisco Secure ACS 3.2 is now capable of processing multiple LDAP authentication requests in parallel, as opposed to the sequential processing mechanism employed in pre-3.2 versions. This feature greatly improves Cisco Secure ACS performance in "task-intensive" configurations such as in wireless deployments.
- *EAP-TLS enhancements*—New EAP-TLS enhancements have been added to Cisco Secure ACS 3.2 that further extend Cisco Secure ACS PKI capabilities. EAP-TLS authentication against ODBC user databases and EAP-TLS silent-session-resume support are among the new added capabilities. Similar to the PEAP silent session resume, EAP-TLS silent session resume prevents users from reauthenticating during a RADIUS session timeout. This feature is particularly advantageous in wireless applications where users are constantly mobile. The duration of the EAP-TLS silent session timeout is configurable from the Cisco Secure ACS GUI.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1017
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14-846
A-

- *Machine authentication support*—Cisco Secure ACS 3.2 adds the 802.1X machine authentication option using either PEAP with MSCHAPv2 implementation (PEAP-EAP-MSCHAPv2) or EAP-TLS. Machine authentication is used at boot time to authenticate and communicate with Windows domain controllers when connecting to 802.1X secure ports. Machine authentication allows pulling down machine group policies from the Windows Active Directory independent of a subsequent interactive user authentication session.
- *EAP mixed configurations*—Cisco Secure ACS 3.2 now supports the following EAP types: PEAP-EAP-GTC (Cisco PEAP), PEAP-EAP-MSCHAPv2 (Microsoft PEAP), EAP-TLS, EAP message digest algorithm 5 (MD5), and Cisco EAP Wireless (LEAP). Cisco Secure ACS 3.2 allows flexible EAP settings (one or several EAP types can be selected concurrently), allowing Cisco Secure ACS to intelligently process EAP authentications, depending on the nature of the 802.1X supplicant presented by the end users.
- *Accounting support for Cisco Aironet wireless access points*—Cisco Secure ACS 3.2 now supports user-based accounting from Cisco Aironet wireless access points when they are configured as RADIUS (Cisco Aironet Access Point) AAA clients.
- *Downloadable access control lists (ACLs) for VPN users*—Cisco Secure ACS 3.2 extends per-user access-control-list support to Cisco VPN solutions (in addition to the current support for Cisco PIX® Firewall solutions). With this option, administrators can define ACLs of any length, for a user or group of users within the Cisco Secure ACS GUI. Cisco VPN 3000 Concentrator v4.0 is required for this feature.

Cisco Secure ACS Benefits

Cisco Secure ACS is a powerful access control server with many high-performance and scalability features for any organization growing its WAN or LAN connectivity:

- *Ease of use*—A Web-based user interface simplifies and distributes configuration for user profiles, group profiles, and Cisco Secure ACS configuration.
- *Scalability*—Cisco Secure ACS is built to support large networked environments with support for redundant servers, remote databases, and user database backup services.
- *Extensibility*—LDAP authentication forwarding supports the authentication of user profiles stored in directories from leading directory vendors, including Sun, Novell, and Microsoft.
- *Management*—Windows Active Directory and Windows NT database support consolidates Windows username and password management, and uses the Windows Performance Monitor for real-time statistics viewing.
- *Administration*—Different access levels for each Cisco Secure ACS administrator—and the ability to group network devices—enable easier control and maximum flexibility to facilitate enforcement and changes of security policy administration over all the devices in a network.
- *Product flexibility*—Because Cisco IOS® Software has embedded support for AAA, Cisco Secure ACS can be used across virtually any network access server that Cisco sells. (The Cisco IOS Software release must support RADIUS or TACACS+.)
- *Protocol flexibility*—Cisco Secure ACS includes simultaneous TACACS+ and RADIUS support for a flexible solution with VPN or dial support at the origin and termination of IP Security (IPSec) and Point-to-Point Tunneling Protocol (PPTP) tunnels.
- *Integration*—Tight coupling with Cisco IOS routers and VPN solutions provides features such as Multichassis Multilink Point-to-Point Protocol and Cisco IOS command authorization.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1018
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.845
A.

- *Third-party support*—Cisco Secure ACS offers token server support for any OTP vendor that provides an RFC-compliant RADIUS interface (such as RSA, PassGo, Secure Computing, ActiveCard, Vasco, and CryptoCard).
- *Control*—Cisco Secure ACS provides dynamic quotas for time-of-day, network usage, number of logged sessions, and day-of-week access restrictions.

System Requirements

Cisco Secure ACS is available in two options: Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine—a 1-RU security-hardened appliance with a preinstalled Cisco Secure ACS license

Hardware Requirements

For implementation of Cisco Secure ACS Windows, your Windows Server must meet the following minimum hardware requirements:

- Pentium processor, 550 MHz or faster
- 256 MB RAM
- 250 MB free disk space, more if you are running your database on the same device
- Minimum resolution of 800 x 600 with 256 colors

The Cisco Secure ACS Solution Engine is available on a Cisco 1111 platform with the following specifications:

- Pentium IV processor, 2.66 GHz
- 1 GB RAM
- 40 GB free disk space
- 2 built-in 10/100 Ethernet controllers
- 1 floppy disk drive
- 1 CD-ROM drive

Device and User Directory Compatibility

A complete list of minimum system and software requirements for devices, browsers, and user directories compatible with Cisco Secure ACS 3.2 is found in the *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS v3.2* document published with Cisco Secure ACS v3.2 user guides.

Ordering Information

Cisco Secure ACS is available for purchase through regular Cisco sales and distribution channels worldwide. Cisco Secure ACS Windows includes all the necessary components needed for an independent installation on a Microsoft Windows workstation. Cisco Secure ACS Solution Engine is shipped with a preinstalled Cisco Secure ACS software license.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1019
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

For More Information

For more information about Cisco Secure ACS 3.2, including the user guide and release notes for the Cisco Secure ACS Version 3.2, visit: http://www.cisco.com/go/acs.

For information about specific product functions or technical questions, send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

For questions about product ordering, availability, and support contract information, send e-mail to the product marketing group at ciscoworks@cisco.com.

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, Catalyst, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203051/ETMG_04/03

ECT/MS CN
CPMI CORREIOS
Fls. Nº 1020
3690
Doc

14.843
A.

Switch Tipo 5 doc 3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1021
3690
Doc.

Rebranding the VPN Client software

This chapter explains how to replace the Cisco Systems brand with your own organization's brand so that when you install and launch the VPN Client software, you see your own organization name, program name, and application names on menus, windows, dialogs, and icons. It also explains how to set up the software so that your users can install it automatically without being prompted to reboot. This feature is called *silent install.*

To rebrand the VPN Client software, you create your own distribution image combining the following elements, which this chapter describes:

- Cisco Systems image that you receive on the Cisco Systems software distribution CD.
- An `oem.ini` file that you create.
- Your own bitmap and icon files to replace the Cisco Systems brand.
- A `vpnclient.ini` file for configuring the VPN Client software globally (see Chapter 2, "Preconfiguring the VPN Client for remote users").
- Individual profile (.pcf) files for each connection entry (see Chapter 2, "Preconfiguring the VPN Client for remote users").
- `setup.bmp` — a bitmap file that displays on the first InstallShield® screen when you install the VPN Client.

These elements should all be in the same directory and folder. Because some of the files may be too large to distribute the oem software on diskettes, we recommend that you make a CD ROM distribution image.

Rebranding takes place when the VPN Client and installation program see a text file called `oem.ini` on your distribution image. The `oem.ini` file is patterned after Microsoft standard initialization files. You create the `oem.ini` file and supply your own text, bitmap files, and icon files. When present, the `oem.ini`, bitmap, and icon files are read when you first start the VPN Client. Since the VPN Client software reads these files when it first starts, the changes from them take effect only *after* you restart the VPN Client applications.

This chapter covers the following topics:

- Areas affected by branding
  - Installation bitmaps
  - Program menu titles and text
  - VPN Dialer
  - Log Viewer
  - Certificate Manager
- Creating the oem.ini file

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1022
3690
Doc.

- Additional Bitmap — setup.bmp

Areas affected by branding

Branding replaces the following screen text, bitmaps, and icons.

- Brand names on windows and dialog boxes.
- Product names on windows and dialog boxes.
- Organization logo on all wizard windows.
- Icons on the user authentication dialog boxes, the system tray (at the bottom right of the screen), desktop (shortcut), status messages, Set MTU window, Log View windows, and Certificate Manager windows.

Installation bitmaps

The InstallShield uses two bitmaps when installing the VPN Client software: the setup bitmap (`setup.bmp`), and the wizard bitmap (`wizard.bmp`).

Figure 4-1 shows the setup bitmap that displays as the first screen during installation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1023
3690
Doc.

14.390
A.

Figure 4-1 Setup bitmap

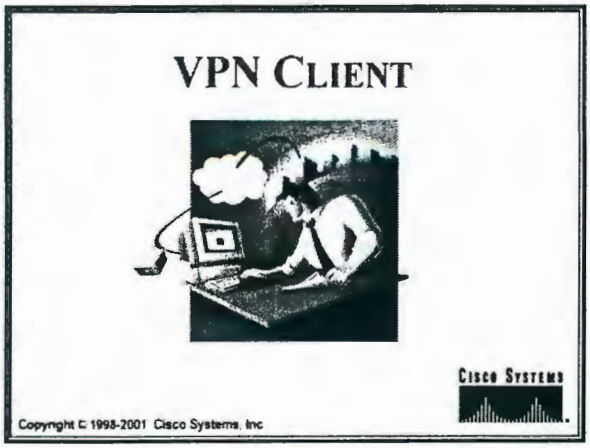
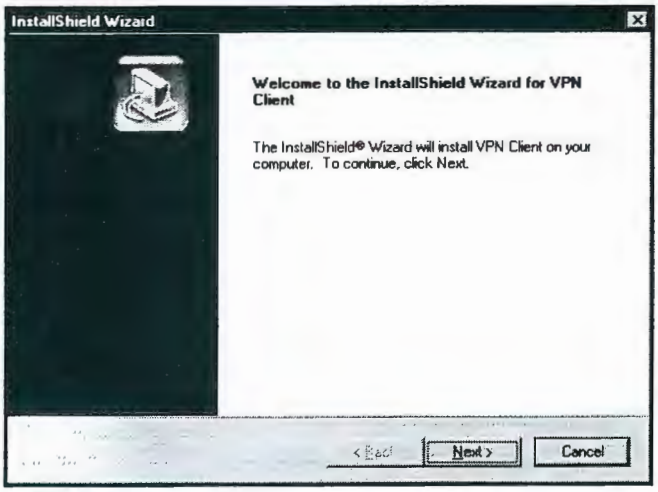


Figure 4-2 shows the wizard bitmap that displays on windows during installation.

Figure 4-2 Wizard bitmap during installation.



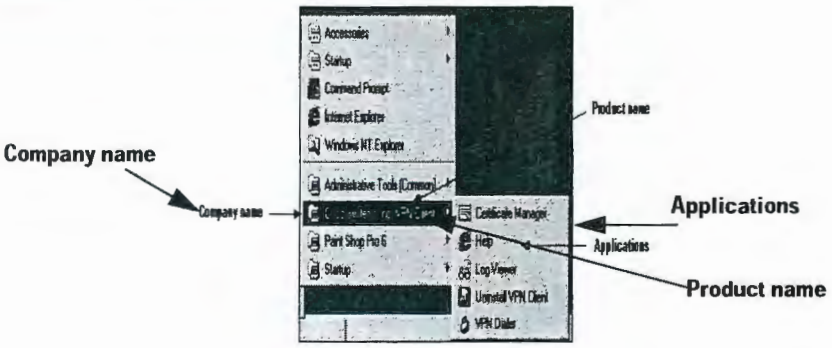
Program menu titles and text

After installation, the organization (company), product, and application names appear in the Cisco Systems VPN Client applications menu (Figure 4-3).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1024
3690
Doc.

14.839
A.

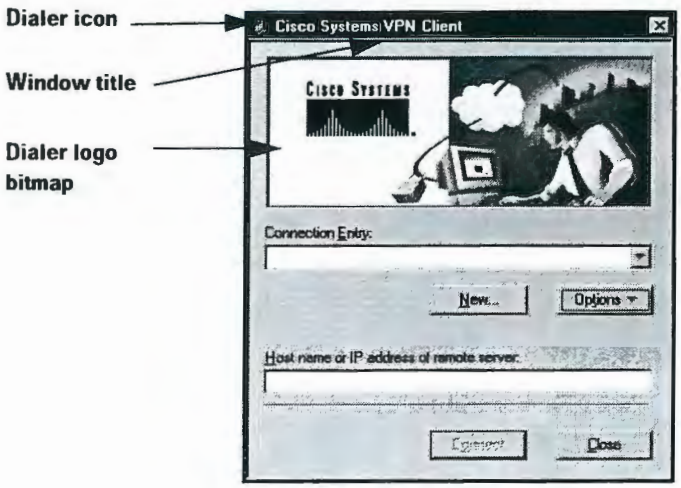
Figure 4-3 Applications menu



VPN Dialer

Figure 4-4 shows a dialer icon, window title, and dialer logo bitmap that the `oem.ini` file replaces in the VPN dialer software.

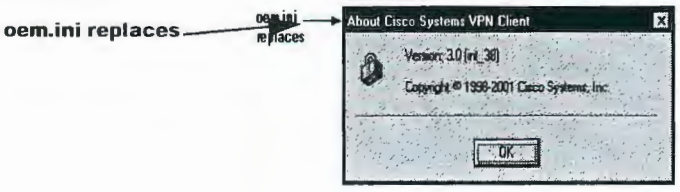
Figure 4-4 Three types of branding changes



When you click the icon in the title line and select **About Cisco Systems VPN Client**, you see information about the copyright and version number of the VPN Client. The `oem.ini` file replaces the window title and the icon. Also the window displays `(OEM)` when you are using the OEM version of the client software (Figure 4-5).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1025
3690
Doc.

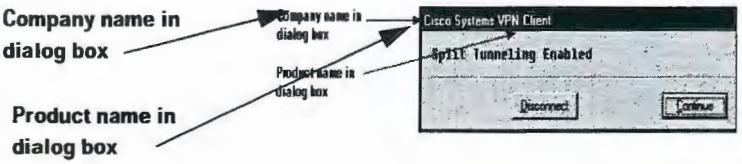
Figure 4-5 About VPN Client



Window titles and text

Figure 4-6 is typical of dialog boxes showing status messages throughout. You can replace "Cisco Systems" with your organization's name and "VPN Client" with a different name for the client application.

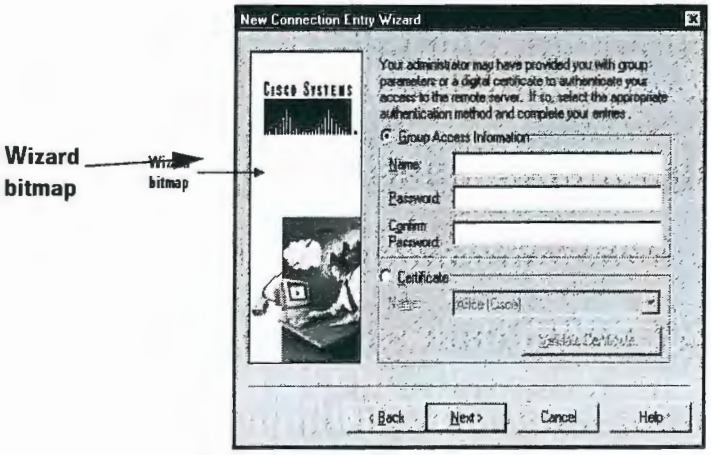
Figure 4-6 Window titles in a dialog box



Bitmaps

The VPN Dialer application displays the wizard bitmap on windows while connecting to a VPN device. Figure 4-7 shows the wizard bitmap as used in the connection wizard.

Figure 4-7 Connection wizard logo



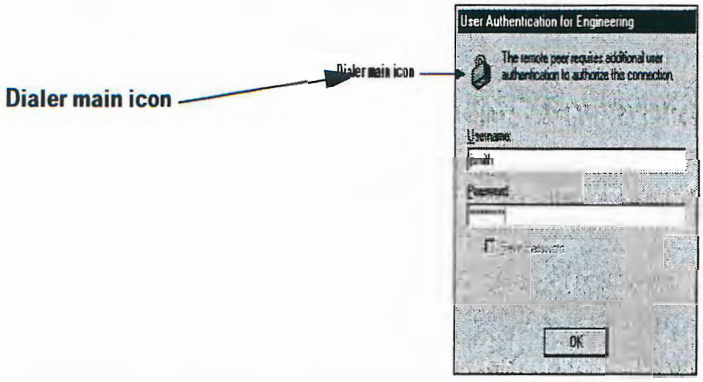
Icons

The next set of figures show the icons used in the VPN Dialer application. You can use the `oem.ini` file to replace all icons with icons you design for your organization. The interface uses several icon (`.ico`) files. The basic size is 32x32 pixels, such as the User Authentication window (Figure 4-8). The operating system automatically condenses the 32x32 icon to fit the 16x16 size displayed on window titles and the system tray (Figure 4-4 and Figure 4-9).

RQS nº 03/2005 - CN
CPMI CORREIOS
1026
3690
Doc.

14.831 A.

Figure 4-8 Dialer icon on User Authentication window

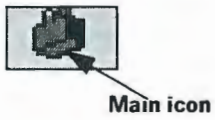


The smaller icon on the system tray appears at the bottom right section of your screen.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1027
3690
Doc.

14-836 A.

Figure 4-9 Icon on system tray



Four icons display while the VPN Dialer is connecting to the Concentrator (Figure 4-10, Figure 4-11, Figure 4-12, and Figure 4-13).

Figure 4-10 Start of negotiation

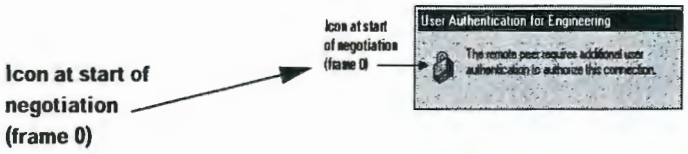


Figure 4-11 First change

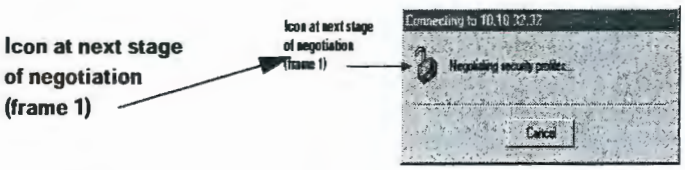


Figure 4-12 Second change

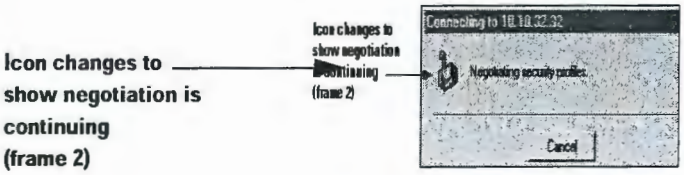
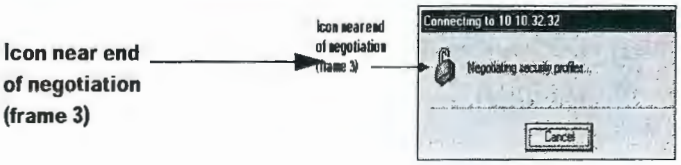


Figure 4-13 Third change

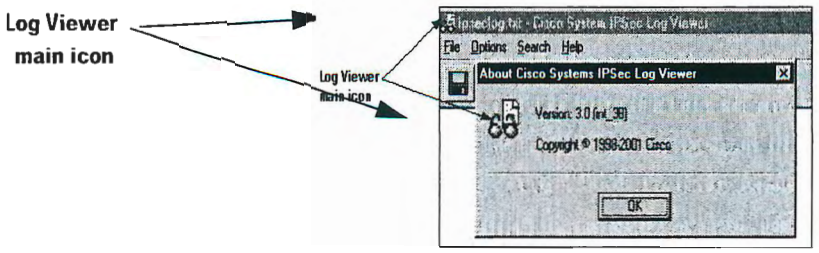


Log Viewer

The Log Viewer section of the oem.ini file replaces the icon used in the Log Viewer application (Figure 4-14). You can also replace the name of the application.

RQS nº 03/2005 - CN
CPMI 1028 CORREIOS
Fls. Nº 3690
Doc.

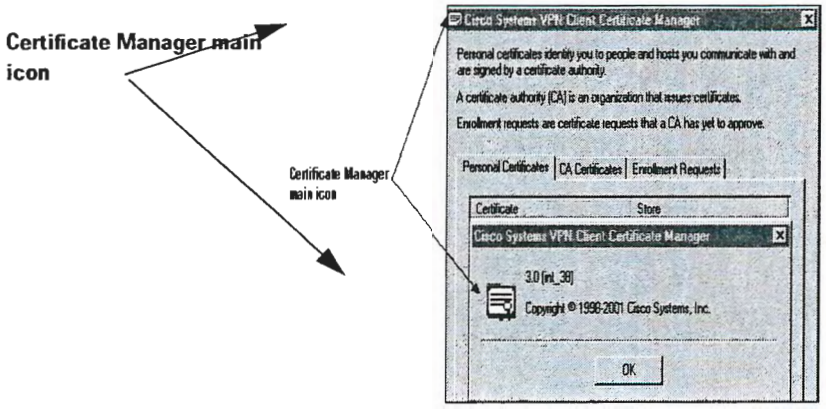
Figure 4-14 Log Viewer icon



Certificate Manager

The Certificate Manager section of the oem.ini file replaces the icon used in the Certificate Manager application (Figure 4-15). You can also replace the name of the application.

Figure 4-15 Certificate Manager icon



Dealing with incompatible GINAs

Cisco's Graphical Identification and Authentication (GINA) program (DLL) is incompatible with some third party GINAs, such as PAL Gina. When an incompatibility exists, the Cisco GINA does not install. The VPN Dialer starts to come up, checks to see if the GINA is compatible, and if not comes up without the presence of a GINA. If your site is using its own or a third party GINA, you can specify the name of the GINA in the `oem.ini` file so that the installation program can identify it when it checks for incompatible GINAs. To do this, include the `IncompatibleGinas` parameter in the `oem.ini` file (see oem.ini file keywords and values).

Creating the oem.ini file

Your distribution CD must contain the `oem.ini` file to execute the branding changes. The `oem.ini` file contains the locations and names of bitmaps, icons, window titles, and screen text needed for OEM branding, all of which need to be in the same directory. When you install or start the VPN Client, the software checks to see if there is an `oem.ini` file. If so, the software scans it for bitmaps, icons, and text.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1029
3690
Doc

If the oem.ini file lacks an element (for example, text for the product name), then the software uses whatever you have specified in the default section of the file. If no oem.ini file exists, the software defaults to Cisco Systems bitmaps, icons, and text.

Use Notepad or another ASCII text editor to create the oem.ini file and enter brand text and the names of your bitmap and icon files. See Table 4-1.

The format of the oem.ini file is the same as a standard Windows ini file:

- Use a semicolon (;) to begin a comment.
- Set values by entering keyword=value.
- If you don't specify a value for a keyword, the application uses the default.
- Keywords are not case-sensitive, but using upper- and lowercase makes them more readable.

Sample oem.ini file

```
; This is a sample oem.ini file that you can use to overwrite Cisco Systems
; brand name on windows,bitmaps, and icons with your organization's brand
; name.
;
; This file has six sections: [Main],[Brand], [Default], [Dialer],
; [Log viewer], and [Configuration Manager]. Each section has keywords
; designating parts of the interface that the file replaces.
;
; The [Main] section specifies incompatible GINAs.

[Main]
IncompatibleGinas=PALGina.dll

; The [Brand] section controls window titles during installation and in the
; destination folder for the product and applications.
;
[Brand]

CompanyText = Wonderland University

ProductText = Wonderland Client

;
; The default section establishes the default bitmap and icon to use if
; assignments are left blank. WizardBitMap appears in installation and
; connection wizards. This section also sets up silent installation.
; Silent mode installation proceeds without user intervention.
;
[Default]
WizardBitMap = wuwiz.bmp
MainIcon = wudial.ico
SilentMode = 1
InstallPath = C:\Program Files\Wonderland University\Wonderland Client
DefGroup = Wonderland Client
Reboot = 1
;
; The [Dialer] section controls the text and icons for the dialer software.
; AppNameText appears on the application selection menu. DialerBitMap
; appears on connection windows.
;
[Dialer]

AppNameText = Wonderland Dialer

DialerBitMap = wudial.bmp

MainIcon = wudial.ico

Frame0Icon = wudial.ico
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1030
Doc. 3690

```
Frame1Icon = wudial1.ico
Frame2Icon = wudial2.ico
Frame3Icon = wudial3.ico
;
; The [Log viewer] section controls the text and icons for the Log Viewer
; application. AppNameText appears on the application selection menu and
; the title screen. MainIcon appears on the window title bar and About
; dialog.
;
[Log viewer]
AppNameText = Wonderland LogViewer
MainIcon = log.ico
;
; The [Certificate Manager] section controls the text and icon for the
; Certificate Manager application. AppNameText appears on the application
; selection menu and the title screen. MainIcon appears on the window title
; bar.
;
[Certificate Manager]
AppNameText = Wonderland Certificate Manager
MainIcon = cm.ico
```

oem.ini file keywords and values

Table 4-1 describes each part of the `oem.ini` file.

Table 4-1 oem.ini file parameters

Keyword	Description	Value
`[Main]`	Optional field to identify a section of the OEM.ini file to address special circumstances	Keep exactly as shown.
`IncompatibleGinas=`	Lists Graphical Identification and Authentication dynamic link libraries (GINA.DLLs) that are incompatible with Cisco's GINA.	After the keyword and equal sign, enter the name(s) of the GINAs, separated by commas. Enclose each GINA within quotes. For example: IncompatibleGinas= "PALGina.dll", "Ourgina.dll"
`[Brand]`	Required field to identify the branding text that appears on window titles and descriptions throughout the client application.	Keep exactly as shown, as the first branding section of the file.
`CompanyText=`	Keyword that identifies the name of your organization. If not present, the default is "Cisco Systems."	After the keyword and equal sign, enter the organization's name. The name can contain spaces and is not case sensitive.
`ProductText=`	Keyword that identifies the name of the application. If not present, the default is "VPN Client."	After the keyword and equal sign, enter the product name. The name can contain spaces and is not case sensitive.
`[Default]`	Required field to identify the section that contains names of default bitmap and icon to use if values are blank.	Enter exactly as shown, as the second section of the file.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº
1031
Doc 690

14.834 A

Table 4-1 oem.ini file parameters (continued)

Keyword	Description	Value
WizardBitMap=	Keyword that identifies the vertical graphic that appears on the side of some VPN Client windows, such as the Setup Installation windows and the Connection window (Figure 4-7). The Cisco Systems vertical graphic is 104x249 pixels; 256 colors.	After the keyword and equal sign, enter the name of the wizard bitmap file.
MainIcon=	Keyword that identifies the main icon to use as a default. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the default icon file. You need to create only the 32x32 size.
SilentMode=	Keyword that identifies whether or not to activate silent installation.	After the keyword and equal sign, enter either 0 or 1. 1 activates silent installation: 0 = prompt the user during installation. 1= do not prompt the user during installation.
InstallPath=	Keyword that identifies the directory into which to install the client software.	After the keyword and equal sign, enter the name of the directory in the suggested format: *root:\programs\company\product*
DefGroup=	Keyword that identifies the name of the folder to contain the client software.	After the keyword and equal sign, enter the name of the destination folder in the suggested format: *foldername*
Reboot=	Keyword that identifies whether or not to restart the system after the silent installation. If SilentMode is on (1) and Reboot is 1, the system automatically reboots after installation finishes.	After the keyword and equal sign, enter 0, 1, or 2: 0 = display the reboot dialog. 1 (and SilentMode = 1) = automatically reboot the system when installation finishes. 2 (and SilentMode = 1) = do not reboot after installation finishes.
[Dialer]	Required field to identify the section that contains the name of the Dialer application, the bitmap to use on the connections window, and the connection icons.	Enter exactly as shown, as the third section of the file.
AppNameText=	Keyword that identifies the name of the dialer application.	After the keyword and equal sign, enter the name of the dialer application. The name can contain spaces and is not case sensitive.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1032
3690
Doc.

Table 4-1 oem.ini file parameters (continued)

Keyword	Description	Value
DialerBitMap=	Keyword that identifies the dialer bitmap (shown in Figure 4-4). The dimensions of this bitmap are 298x116 pixels; 256 colors.	After the keyword and equal sign, enter the name of the dialer bitmap file.
MainIcon=	Keyword that identifies the primary icon file for the connection and authorization windows. This icon appears in the User Authentication window and the system tray, for example (Figure 4-8 and Figure 4-9). You can rotate or flip the lock image to fit with the brand graphic. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the primary icon file. The User Authentication window uses the 32x32 size and the system tray uses the 16x16 size. You need to create only the 32x32 size.
Frame0Icon=	Keyword that identifies the Frame 0 icon file, which is based on the main icon (Figure 4-10). This icon shows at the start of the connection negotiation. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame0 icon file.
Frame1Icon=	Keyword that identifies the Frame 1 icon file, which is based on the main icon (Figure 4-11). This icon shows further progress of the connection. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame1 icon file.
Frame2Icon=	Keyword that identifies the Frame 2 icon file, which is based on the main icon (Figure 4-12). This icon shows further progress of connection establishment. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame2 icon file.
Frame3Icon=	Keyword that identifies the Frame 3 icon file, which is based on the main icon (Figure 4-13).This icon shows the end of connection establishment. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame3 icon file.
[Log viewer]	Required field to identify the application name and icon for the Log Viewer application.	Keep exactly as shown, as the fourth section of the file.
AppNameText=	Keyword that identifies the name of the Log Viewer application.	After the keyword and equal sign, enter the name you want to give to the Log Viewer application. The name can contain spaces and is not case sensitive.
MainIcon=	Keyword that identifies the icon for the Log Viewer title bar, About window and applications menu. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign enter the name of the icon (.ico) file for this icon. You need to create only the 32x32 size.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1033
Doc. 3690

Table 4-1 oem.ini file parameters (continued)

Keyword	Description	Value
[Certificate Manager]	Required field to identify the application name and icon for the Certificate Manager application.	Keep exactly as shown, as the sixth section of the file.
AppNameText=	Keyword that identifies the name of the Certificate Manager application.	After the keyword and equal sign, enter the name you want to give to the Certificate Manager application. The name can contain spaces and is not case sensitive.
MainIcon=	Keyword that identifies the icon for the Configuration Manager title bar and the applications menu. The dimensions are 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the icon (.ico) file for this icon.

Installing the VPN Client without user intervention (silent mode)

To install the VPN Client software without user intervention, you can use a feature called *silent mode*. To implement silent mode with or without rebranding, you can create an `oem.ini` file containing only the part that configures silent mode. In this file, you turn SilentMode on, identify the pathname and folder to contain the VPN Client software, and reboot the system, all without user interaction.

Here is a sample `oem.ini` file for implementing silent mode:

```
[Default]
SilentMode = 1
InstallPath = C:\Program Files\Engineering\IPSec Connections
DefGroup = IPSec remote users
Reboot = 1
```

Table 4-2 oem.ini file silent mode parameters

.ini parameter (keyword)	Parameter Description	Values
SilentMode=	Keyword that identifies whether or not to activate non interactive installation.	After the keyword and equal sign, enter either 0 or 1. 1 activates silent installation: 0 = prompt the user during installation. 1= do not prompt the user during installation.
InstallPath=	Keyword that identifies the directory into which to install the client software.	After the keyword and equal sign, enter the name of the directory in the suggested format: *root:\programs\organization\product*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1034
3690
Doc.

Table 4-2 oem.ini file silent mode parameters (continued)

.ini parameter (keyword)	Parameter Description	Values
`DefGroup=`	Keyword that identifies the name of the folder to contain the client software.	After the keyword and equal sign, enter the name of the destination folder in the suggested format: *foldername*
`Reboot=`	Keyword that identifies whether or not to restart the system after the silent installation. If SilentMode is on (1) and Reboot is 1, the system automatically reboots after installation finishes.	After the keyword and equal sign, enter 0, 1, or 2: 0 = display the reboot dialog. 1 (and SilentMode = 1) = automatically reboot the system when installation finishes. 2 (and SilentMode = 1) = do not reboot after installation finishes.

Additional Bitmap — setup.bmp

The oem version of VPN Client includes a bitmap on the distribution CD that is not in the `oem.ini` file: `setup.bmp`. You can substitute your own image for this .bmp file, as long as you keep the current filename (`setup.bmp`) and make sure that the file is in the same directory and folder as the `oem.ini` file.

`setup.bmp` displays a logo on the window when you start the installation program. The size of the Cisco Systems setup bitmap is 330x330 pixels and it uses 256 colors.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1035
Fls. Nº
3690
Doc.

14.828
A.

Job Title: 6C4 IBM eServer pS 30 Model

Time Queued: Tr 24 04:16:25 2003
Time Printed: Tr 24 05:12:23 2003

Submitted By: cmaciel

Need help? Call your local NCO HelpDesk.

PIO_DEV brbrap7a#ibmNetPrinter (ibm4320) @ brbraprt01

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1036
3690
Doc.

14.827
A.

- Height: 172.8 mm (06.8 in)
- Weight:
  - 32.0 kg (70.4 lb) - Minimum Configuration
  - 47.3 kg (104 lb) - Maximum Configuration with rails

Operating Environment

- Temperature: 5 to 35 degrees C (41 to 95 F)
- Relative humidity: 8% to 80%
- Maximum wet bulb: 27 degrees C (80 F)
- Operating voltage: (auto-ranging) 100 to 127 or 200 to 240 V ac
- Operating frequency: 50/60 Hz
- Power requirements:
  - 2-way (typical configuration): 330 watts
  - 2-way (maximum configuration): 500 watts
  - 4-way (typical configuration): 500 watts
  - 4-way (maximum configuration): 750 watts
- Thermal output:
  - 2-way (typical configuration): 1129 BTU/hour
  - 2-way (maximum configuration): 1693 BTU/hour
  - 4-way (typical configuration): 1693 BTU/hour
  - 4-way (maximum configuration): 2540 BTU/hour
- Power source loading:
  - 2-way (typical configuration): 0.348 kVA
  - 2-way (maximum configuration): 0.522 kVA
  - 4-way (typical configuration): 0.522 kVA
  - 4-way (maximum configuration): 0.783 kVA
  - Maximum altitude: 2,135 m (7,000 ft)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1037
3690
Doc.

Noise Level and Sound Power

- Sound Power: Model 6C4 6.0 Bels Idle/6.0 Bels Operating

EMC Conformance Classification

- This equipment is subject to FCC rules and it shall comply with the appropriate FCC rules before final delivery to the buyer or centers of distribution.
  - U.S.A.: FCC Class A for Rack Mount
  - Europe: CISPR 22 Class A for Rack Mount
  - Japan: VCCI-A for Rack Mount
  - Korea: Korean Requirement Class A for Rack Mount
  - China: People's Republic of China commodity inspection law

Homologation – Telecom Environmental Testing (Safety and EMC)

- Homologation approval for specific countries has been initiated with the IBM Homologation and Type Approval (HT&A) organization in LaGaude. These IBM pSeries models and applicable features meet the environmental testing requirements of the country TELECOM and have been designed and tested in compliance with the Full Quality Assurance Approval (FQAA) process as delivered by the British Approval Board for Telecom (BABT), the U.K. Telecom Regulatory authority.

Product Safety/Country Testing/Certification

- UL 1950 Underwriters Laboratory, Safety Information

roriz@IBM-297NYWD11S3

14-826
4

Job Title: SWITCH_TIPO5_doc4.pdf

Time Queued: Thu Jul 24 04:18:46 2003
Time Printed: Thu Jul 24 05:12:45 2003

Submitted By: roriz@IBM-297NYWD11S3

roriz@IBM-297NYWD11S3

Need help? Call your local NCO HelpDesk.

PIO_DEV: ibm@brbrap7a#ibmNetPrinter (ibm4320) @ brbraprt01

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1038
3690
Doc.

Cisco Systems

14.825
A.

Data Sheet

Cisco **VPN** Client

Supports Easy VPN Remote

Introduction

The Cisco® VPN Client is software that enables customers to establish secure, end-to-end encrypted tunnels to any Cisco Easy VPN server. This thin design, IP Security (IPsec) compliant implementation is available from Cisco.com for customers with SMARTnet® support, and is included free of charge with the Cisco VPN 3000 Concentrator. The client can be preconfigured for mass deployments and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management.

The Cisco VPN Client provides support for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit) and Mac OS X 10.2 (Jaguar).

The Cisco VPN Client is compatible with the following Cisco products (Cisco Easy VPN servers):

- Cisco VPN 3000 Series Concentrator Software Version 3.0 and later
- Cisco IOS® Software Release 12.2(8)T and later
- Cisco PIX® Firewall Software Version 6.0 and later

Features and Benefits

- Support for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit) and Mac OS X 10.2 (Jaguar).
- VPN Virtual Interface Adapter present on Windows 2000 and XP
- System coexistence with Microsoft L2TP/IPsec client
- MSI (Windows Installer) package available for NT, 2000, and XP
- Intelligent peer availability detection (DPD)
- Simple Certificate Enrollment Protocol (SCEP)
- Data compression (LZS)
- Command-line options for connecting, disconnecting, and connection status
- Configuration file with option locking
- Support for Microsoft network login (all platforms)
- Domain Name System (DNS) including DDNS/DHCP computer name population, Split DNS,
- Windows Internet Name Service (WINS), and IP address assignment
- Load balancing and backup server support

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1039
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14824
A.

- Centrally controlled policies (including backup server list)
- Integrated personal firewall (stateful firewall): Zone Labs technology—Windows only
- Personal firewall enforcement: Cisco Security Agent, BlackIce, Sygate, Zone Alarm—Windows only
- Integration with the iPass remote access client software, including: one-click (single sign-on), VPN auto-teardown, and Windows pre-login support—Windows only.
- Client connection auto initiation for wireless LAN environments

Cisco Easy VPN

Cisco Easy VPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies VPN deployment for remote offices and teleworkers. Based on the Cisco Unified Client Framework, Cisco Easy VPN centralizes VPN management across all Cisco VPN devices thus reducing the complexity of VPN deployments. Cisco Easy VPN enables an integration of VPN remotes—Cisco routers, PIX firewalls, Cisco VPN concentrators or software clients—within a single deployment with a consistent policy and key management method thus simplifying remote side administration.

Table 1 Product Specifications

Description	Specification
Operating Systems	Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 & 64-bit) and Mac OS X 10.2 (Jaguar).
Tunneling Protocols	IPSec Encapsulating Security Payload (ESP), PPTP, L2TP, L2TP/IPSec, Network Address Translation (NAT) Transparent IPsec, Ratified IPsec/UDP (with autodetection and fragmentation avoidance), IPsec/TCP
Encryption/Authentication	IPsec (ESP) using Data Encryption Standard (DES)/Triple DES (3DES) (56/168-bit) or AES (128/256-bit) with MD5 or SHA
Key Management	Internet Key Exchange (IKE) —Aggressive and Main Mode (Digital certificates) Diffie-Hellman (DH) Groups 1, 2, and 5 Perfect Forward Secrecy (PFS) Rekeying
Data Compression	Lempel-Ziv standard (LZS) compression
Digital Certificates	The supported enrollment mechanisms are Simple Certificate Enrollment Protocol (SCEP) and Certificates enrolled with Microsoft Internet Explorer. Supported certificate authorities (CAs) include: Entrust, Netscape, Baltimore, RSA Keon, Verisign, and Microsoft. Entrust ESP and Entelligence Client support. Smartcards: Supported via MS CAPI (CRYPT_NOHASHOID) include: Activcard (Schlumberger cards), Aladdin, Gemplus and Datakey.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1040
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

14.823
SA.

Table 1 Product Specifications

Description	Specification
Authentication	Extended Authentication (XAUTH) Remote Authentication Dial-In User Service (RADIUS) with support for – State/Reply-Message attributes (token cards), – Kerberos/Active Directory authentication—new in 4.0 – Security Dynamics (RSA SecurID Ready) – Microsoft NT Domain authentication – MSCHAPv2 - NT Password Expiration – X.509v3 digital certificates External user authorization information may be obtained via LDAP or RADIUS—new in 4.0
Profile Management	Client can be easily distributed with preconfigured Profile Configuration Files (PCFs)
Policy Management	ISAKMP Configuration Method (Mode-Config) centrally controlled policies including DNS/Split DNS, WINS, IP Address, and Default Domain Name. Ability to save connection password, split tunneling/ local LAN access control/ networks, remote access load balancing, Centralized Protection Policy (firewall), personal firewall requirement (Are You There?), software update notification

Table 2 Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco PIX Firewall	Cisco IOS
Version used for Feature Chart	4.0	6.3	12.2(13)T
All Cisco Easy VPN Client OS Support	Y	Y	Y
Certicom/Netlock Compatibility Tested	Y	N	N
Basic Client Functionality			
DES/3DES, MD5/SHA	Y	Y	Y
AES (128, 256 bit)	Y	Y	Y
PreShared Secret (Group)	Y – Int & Ext	Y – Int & Ext	Y – Int
DNS, WINS, Default Domain, IP	Y	Y	Y
Split DNS Support	Y	N	N
Dynamic DNS/DHCP (Computer name population)	Y	N	N
Connection auto-initiation	Y	Y	Y
Authentication			
RADIUS	Y	Y	
RADIUS with State+Reply Tokens	Y	Y	Y

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1041
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco PIX Firewall	Cisco IOS
RADIUS with NT Password Expire	Y	N	Y
Native RSA SecurID (SDI)	Y	N	N
Kerberos/Active Directory	Y	N	N
Native NT Domain	Y	N	N
Certificate/Entelligence/Smartcard	Y	Y	Y
Peer Detection (DPD)	Y	Y	Y
Backup Server List (Client)	Y	Y	Y
Backup Server List (Central Control)	Y	N	N
Rekeying	Y	Y	Y
Idle Timeout Support	Y	Y	N
Max Connection Limit	Y	Y	N
User IP Filters	Y	N	Y through ACLs
RADIUS Group Lock	Y	N	N
Address Assignment			
Internal Address Pool	Y	Y	Y
DHCP	Y	N	N
RADIUS	Y	N	N
Advanced Functionality			
Data Compression	Y	N	Y
Concentrator Banner Message	Y	N	N
Software Update Notification	Y	N	N
Saved Password Control	Y	N	N
Tunnel Default Gateway	Y	N	N
Clustering / Load Balancing	Y	N	N
Tunneling Methods			
All Tunneling / Split Tunneling	Y	Y	Y
Local LAN Access Permission	Y	N	N
Ratified IPSec/UDP NAT Transparency (including auto-detection and fragmentation avoidance	Y	Y	Y
NAT/PAT Transparency (UDP)	Y	N	N
Extranet IPsec (TCP)	Y	N	N

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1042
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.821
A.

Table 2 Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco PIX Firewall	Cisco IOS
Client Personal Firewall Support			
User Controlled (Always On)	Y	Y	Y
Cisco Security Agent/BlackIce/Sygate/Zone Alarm Enforcement (AYT)	Y	N	N
Centralized Protection Policy (CPP)	Y	N	N
Zone Labs Integrity	Y	N	N

Ordering Information

Where to Buy Cisco Products

Visit http://www.cisco.com/public/ordering_info.shtml

Product and Part Numbers

Available for customers with SMARTnet™ support at

http://www.cisco.com/kobayashi/sw-center/vpn/client.

Part Numbers for the Cisco VPN Client

Description	Part Number
Cisco VPN Client	CVPN-CLIENT-K9=

Documentation

For part numbers for product specific documentation, visit:

http://www.cisco.com/univercd/cc/td/doc/pcat/swdo__d1.htm

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1043
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14-820
A-

Cisco Systems

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. PIX and SMARTnet are trademarks, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW4425 0403

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 1011
Doc. 3690

14.819

Switch Tipo 5 doc 4

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1045
Doc. 3690

Cisco Systems

Data Sheet

Cisco **VPN** Client

Supports Easy VPN Remote

Introduction

The Cisco® VPN Client is software that enables customers to establish secure, end-to-end encrypted tunnels to any Cisco Easy VPN server. This thin design, IP Security (IPsec) compliant implementation is available from Cisco.com for customers with SMARTnet® support, and is included free of charge with the Cisco VPN 3000 Concentrator. The client can be preconfigured for mass deployments and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management.

The Cisco VPN Client provides support for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit) and Mac OS X 10.2 (Jaguar).

The Cisco VPN Client is compatible with the following Cisco products (Cisco Easy VPN servers):

- Cisco VPN 3000 Series Concentrator Software Version 3.0 and later
- Cisco IOS® Software Release 12.2(8)T and later
- Cisco PIX® Firewall Software Version 6.0 and later

Features and Benefits

- Support for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit) and Mac OS X 10.2 (Jaguar).
- VPN Virtual Interface Adapter present on Windows 2000 and XP
- System coexistence with Microsoft L2TP/IPsec client
- MSI (Windows Installer) package available for NT, 2000, and XP
- Intelligent peer availability detection (DPD)
- Simple Certificate Enrollment Protocol (SCEP)
- Data compression (LZS)
- Command-line options for connecting, disconnecting, and connection status
- Configuration file with option locking
- Support for Microsoft network login (all platforms)
- Domain Name System (DNS) including DDNS/DHCP computer name population, Split DNS,
- Windows Internet Name Service (WINS), and IP address assignment
- Load balancing and backup server support

RG/TP 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1046
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.817
A-

- Centrally controlled policies (including backup server list)
- Integrated personal firewall (stateful firewall): Zone Labs technology—Windows only
- Personal firewall enforcement: Cisco Security Agent, BlackIce, Sygate, Zone Alarm—Windows only
- Integration with the iPass remote access client software, including: one-click (single sign-on), VPN auto-teardown, and Windows pre-login support—Windows only.
- Client connection auto initiation for wireless LAN environments

Cisco Easy VPN

Cisco Easy VPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies VPN deployment for remote offices and teleworkers. Based on the Cisco Unified Client Framework, Cisco Easy VPN centralizes VPN management across all Cisco VPN devices thus reducing the complexity of VPN deployments. Cisco Easy VPN enables an integration of VPN remotes—Cisco routers, PIX firewalls, Cisco VPN concentrators or software clients—within a single deployment with a consistent policy and key management method thus simplifying remote side administration.

Table 1 Product Specifications

Description	Specification
Operating Systems	Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 & 64-bit) and Mac OS X 10.2 (Jaguar).
Tunneling Protocols	IPSec Encapsulating Security Payload (ESP), PPTP, L2TP, L2TP/IPSec, Network Address Translation (NAT) Transparent IPsec, Ratified IPsec/UDP (with autodetection and fragmentation avoidance), IPsec/TCP
Encryption/Authentication	IPsec (ESP) using Data Encryption Standard (DES)/Triple DES (3DES) (56/168-bit) or AES (128/256-bit) with MD5 or SHA
Key Management	Internet Key Exchange (IKE) —Aggressive and Main Mode (Digital certificates) Diffie-Hellman (DH) Groups 1, 2, and 5 Perfect Forward Secrecy (PFS) Rekeying
Data Compression	Lempel-Ziv standard (LZS) compression
Digital Certificates	The supported enrollment mechanisms are Simple Certificate Enrollment Protocol (SCEP) and Certificates enrolled with Microsoft Internet Explorer. Supported certificate authorities (CAs) include: Entrust, Netscape, Baltimore, RSA Keon, Verisign, and Microsoft. Entrust ESP and Entelligence Client support. Smartcards: Supported via MS CAPI (CRYPT_NOHASHOID) include: Activcard (Schlumberger cards), Aladdin, Gemplus and Datakey.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1047
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.816
A.

Table 1 Product Specifications

Description	Specification
Authentication	Extended Authentication (XAUTH) Remote Authentication Dial-In User Service (RADIUS) with support for – State/Reply-Message attributes (token cards), – Kerberos/Active Directory authentication—new in 4.0 – Security Dynamics (RSA SecurID Ready) – Microsoft NT Domain authentication – MSCHAPv2 - NT Password Expiration – X.509v3 digital certificates External user authorization information may be obtained via LDAP or RADIUS—new in 4.0
Profile Management	Client can be easily distributed with preconfigured Profile Configuration Files (PCFs)
Policy Management	ISAKMP Configuration Method (Mode-Config) centrally controlled policies including DNS/Split DNS, WINS, IP Address, and Default Domain Name. Ability to save connection password, split tunneling/ local LAN access control/ networks, remote access load balancing, Centralized Protection Policy (firewall), personal firewall requirement (Are You There?), software update notification

Table 2 Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco PIX Firewall	Cisco IOS
Version used for Feature Chart	4.0	6.3	12.2(13)T
All Cisco Easy VPN Client OS Support	Y	Y	Y
Certicom/Netlock Compatibility Tested	Y	N	N
Basic Client Functionality			
DES/3DES, MD5/SHA	Y	Y	Y
AES (128, 256 bit)	Y	Y	Y
PreShared Secret (Group)	Y – Int & Ext	Y – Int & Ext	Y – Int
DNS, WINS, Default Domain, IP	Y	Y	Y
Split DNS Support	Y	N	N
Dynamic DNS/DHCP (Computer name population)	Y	N	N
Connection auto-initiation	Y	Y	Y
Authentication			
RADIUS	Y	Y	Y
RADIUS with State+Reply Tokens	Y	Y	Y

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1048
3650
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14815
A-

Table 2 Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco PIX Firewall	Cisco IOS
RADIUS with NT Password Expire	Y	N	Y
Native RSA SecurID (SDI)	Y	N	N
Kerberos/Active Directory	Y	N	N
Native NT Domain	Y	N	N
Certificate/Entelligence/Smartcard	Y	Y	Y
Peer Detection (DPD)	Y	Y	Y
Backup Server List (Client)	Y	Y	Y
Backup Server List (Central Control)	Y	N	N
Rekeying	Y	Y	Y
Idle Timeout Support	Y	Y	N
Max Connection Limit	Y	Y	N
User IP Filters	Y	N	Y through ACLs
RADIUS Group Lock	Y	N	N
Address Assignment			
Internal Address Pool	Y	Y	Y
DHCP	Y	N	N
RADIUS	Y	N	N
Advanced Functionality			
Data Compression	Y	N	Y
Concentrator Banner Message	Y	N	N
Software Update Notification	Y	N	N
Saved Password Control	Y	N	N
Tunnel Default Gateway	Y	N	N
Clustering / Load Balancing	Y	N	N
Tunneling Methods			
All Tunneling / Split Tunneling	Y	Y	Y
Local LAN Access Permission	Y	N	N
Ratified IPSec/UDP NAT Transparency (including auto-detection and fragmentation avoidance	Y	Y	Y
NAT/PAT Transparency (UDP)	Y	N	N
Extranet IPsec (TCP)	Y	N	N

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1049
Doc. 3690

14.814

Table 2 Remote Access Feature Comparison Chart

	Cisco VPN 3000	Cisco PIX Firewall	Cisco IOS
Client Personal Firewall Support			
User Controlled (Always On)	Y	Y	Y
Cisco Security Agent/Blackice/Sygate/Zone Alarm Enforcement (AYT)	Y	N	N
Centralized Protection Policy (CPP)	Y	N	N
Zone Labs Integrity	Y	N	N

Ordering Information

Where to Buy Cisco Products

Visit http://www.cisco.com/public/ordering_info.shtml

Product and Part Numbers

Available for customers with SMARTnet™ support at

http://www.cisco.com/kobayashi/sw-center/vpn/client.

Part Numbers for the Cisco VPN Client

Description	Part Number
Cisco VPN Client	CVPN-CLIENT-K9=

Documentation

For part numbers for product specific documentation, visit:

http://www.cisco.com/univercd/cc/td/doc/pcat/swdo__d1.htm

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1050
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

14.813
A.

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. PIX and SMARTnet are trademarks, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RP/LW4425 0403

PROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 051
Doc. 3690

14.812
A.

Switch Tipo 5 doc 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1052
Doc. 3690

Q & A
14.811
A.

Cisco Virtual Private Networks Extending the Classic WAN

April 10, 2000

Q. What is the purpose of this announcement?

A. The purpose of this announcement is to communicate Cisco Systems Virtual Private Networking (VPN) solutions and strategy to analysts, media, customers, and channel partners. The key messages Cisco wishes to communicate include:

- Cisco is the market leader and the company to beat in the VPN market
- With the acquisition of Altiga networks, Cisco provides the most complete enterprise VPN solution in the industry
- Cisco is the best vendor partner to help you build an intelligent, self-defending VPN

Q. What are VPNs?

A. A VPN is secure network connectivity deployed on a shared infrastructure with similar policies and performance as a private network. To ensure privacy and network compatibility, VPNs transmit information through an encrypted tunnel. VPNs are an alternative Wide Area Network (WAN) infrastructure, which replaces or augments existing private networks.

Q. Why is Cisco uniquely positioned for leadership in the VPN market?

A. Cisco has the most robust VPN solution set for customers. Cisco is the market leader in site-to-site VPNs, with more than $100 million in VPN-based revenues in 1999. Cisco is currently the No. 1 market leader in global firewall sales, and has more VPN-enabled routers installed than any other vendor.

Cisco has now augmented its existing site-to-site VPN portfolio with market leading remote-access VPN solutions from Altiga Networks. Cisco now has the industry's only truly scalable, end-to-end VPN solution, and this solution is secure, cost effective and easy to manage.

Q. What differentiates Cisco within the site-to-site VPN market?

A. Cisco is the market leader because of the following:

- *Device Integration for a Comprehensive VPN Solution*—Cisco site-to-site VPN solutions integrate all features required for secure, scalable, and reliable VPN deployments in a single device. Many competitive solutions require multiple devices to provide a comprehensive site-to-site VPN solution, which increases deployment complexity. Cisco integrated, single-device, site-to-site VPN solutions simplify network architectures and lower the total cost of ownership of the VPN solution. Key features provided by Cisco VPN solutions for site-to-site VPN deployment include:
  - Tunneling and encryption support using industry-standard protocols such as Internet Protocol Security (IPsec)
  - Strong perimeter security for the VPN, including stateful firewall and intrusion detection provided by Cisco IOS® firewall

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1053
Doc. 3690

Public
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

Cisco Systems

- Application-aware quality of service (QoS) and bandwidth management for VPN transport reliability
- Full Layer 3 routing, including exterior routing protocols such as Border Gateway Protocol (BGP) for Internet/VPN access
- Diverse WAN and local area network (LAN) interfaces for Internet/VPN access and LAN network connectivity

14.810 A-

- *Scalable Performance*—The Cisco range of VPN-optimized routers scale to meet any site-specific VPN deployment requirements from Integrated Services Digital Network (ISDN) to DS3 speeds.
- *Feature Interoperability*—By delivering a comprehensive site-to-site VPN solution in a single device, Cisco VPN-optimized routers ensure greater interoperability of VPN features such as firewall, QoS, and tunneling/encryption than multi-device solutions offered by competitors.
- *Self-Healing VPN*—Cisco VPN-optimized routers utilize the wealth of network resiliency features resident in Cisco IOS software—such as tunnel keep-alives, tunnel endpoint discovery (TED), and dynamic route discovery via generic routing encapsulation (GRE) tunnels—to provide unsurpassed VPN redundancy and dynamic recovery.
- *Investment Protection*—Cisco site-to-site VPN solutions offer LAN/WAN interface and hardware acceleration modularity, as well as a wealth of input/output (I/O) options. This modularity provides investment protection by enabling users to adapt Cisco VPN-optimized solutions for evolving network and scalability requirements.

Q. What is the current portfolio of Cisco site-to-site VPN products?

A. The Cisco site-to-site VPN router portfolio delivers solutions for small office/home office (SOHO) access through central site VPN aggregation, including platforms for fast-emerging cable and digital subscriber line (DSL) access technologies. The table below outlines the Cisco VPN-optimized router portfolio by deployment segment.

Segment	VPN Access Speed/Method	Product
Small office/Home office (SOHO)	Up to 128 Kbps ISDN	Cisco 800 Series
Broadband SOHO	Up to T1 cable or DSL	Cisco UBr900 Series; Cisco 1400 Series
Small Office	Up to T1/E1	Cisco 1700 Series
Branch Office	Up to dual T1/E1	Cisco 2600 Series
Large Branch Office	nxT1/E1	Cisco 3600 Series; Cisco 7120
Central Site	Up to DS3	Cisco 7100 Series; Cisco 7200 Series

Q. Why does the acquisition of Altiga Networks enable Cisco to provide the most comprehensive enterprise VPN solution?

A. The acquisition of Altiga Networks uniquely positions Cisco to provide the most comprehensive VPN solution in the industry because:

- Enterprise customers can now turn to one strategic vendor for a complete VPN offering, including site-to-site and remote access VPN solutions. The Cisco networking prowess and renowned customer support provide the confidence that customers require when implementing a mission-critical VPN.
- Cisco now provides VPN solutions for every price, performance, functionality, and scalability range required by an enterprise. Cisco recognizes that different customers have different requirements—so Cisco provides a broad range of VPN concentrators, router-based solutions, and firewall-based solutions to meet customer needs.
- Cisco provides both narrowband and broadband solutions for Internet, extranet, and remote access VPNs. This flexibility is critical for enterprises with rapidly growing telecommuter and remote workers.
- Cisco enterprise VPN solutions are complemented by an equally strong lineup of service provider VPN offerings.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1054
Doc. 3690

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14.809

Q. Why is Cisco the best vendor partner to provide an intelligent, self-defending VPN?

A. Because VPNs are an extension of the classic WAN—and Cisco is the WAN market leader—Cisco has the most expertise to help an enterprise build an "intelligent, self-defending" VPN. The critical components of this solution include the following:

- Scalable platforms, including robust VPN concentrators and Cisco IOS routers
- Robust security and appliances, including legacy authentication, digital certificate, firewall, encryption, vulnerability scanning, and intrusion-detection solutions
- Management tools that enable administrators to analyze and manage the VPN as part of the overall network
- Critical QoS instrumentation and service monitoring capabilities that enable customers to:
  - Take advantage of content-aware VPNs
  - Monitor network performance relative to VPN service-level agreements (SLAs)

To complement these core solutions, Cisco also delivers industry-leading customer support and leverages relationships with world-class implementation and service-provider partners.

VPN Applications and Architectures

Q. What are the major VPN solutions that customers deploy?

A. VPNs are segmented into two categories:

1. Remote access VPNs for telecommuters and mobile user applications.
2. Site-to-site VPNs for fixed/branch and home office applications.

Q. What are the major VPN architectures that support these solutions?

A. VPNs can be created and deployed by the enterprise or they can be outsourced by an enterprise to a network service provider. In both cases, a set of technologies is deployed to ensure confidentiality of information as it traverses the public Internet or a service provider's trusted IP network.

Q. What are the different components of a VPN?

A. VPNs can be built in a number of different ways with a number of different technologies. The following major components, however, are typically implemented in a VPN solution:

- A tunnel termination gateway: This is the platform that terminates the encrypted tunnels. Important characteristics are the number of tunnels that can be terminated, the bandwidth that can flow through the box, and the number of different protocols and interfaces that are supported.
- Client software (for remote access VPNs): This is the application that resides on the remote terminal (for example the PC of a telecommuter) that initiates and maintains the tunnels that allow access to the enterprise network.
- Advanced VPN Services (for site-to-site VPNs): Services such as QoS, integrated firewall, and service-level validation provide a comprehensive, integrated site-to-site VPN solution.
- Management infrastructure: These are the tools that allow the service provider or enterprise operator /administrator to deploy, manage and monitor the gateways and clients.

Q. What is IPsec? What IPsec support exists in Cisco products?

A. IPsec is an industry-wide standard for assuring the privacy, integrity, and authenticity of information crossing public Internet Protocol (IP) networks. IPsec is becoming widely adopted as a means of implementing VPNs. Cisco fully supports the entire set of Request for Comments (RFCs) describing IPsec and related protocols, including:

- IPsec (RFC 2401-10)
- IPsec Encapsulating Security Payload (ESP) using DES/3DES (RFC 2406)
- IPsec Authentication Header (AH) using MD5 or SHA (RFC 2403-4)
- Internet Key Exchange (IKE) (RFC 2407-9)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1055
Doc. 3690

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

Support for IPsec exists in a wide range of Cisco products, including Cisco IOS routers, Cisco Secure PIX™ firewalls, Cisco VPN 3000 Concentrators, Cisco cable modems, and Cisco DSL solutions.

Q. What is the difference between enterprise edge VPNs and service-provider network VPNs?

A. Enterprise edge VPNs are VPNs in which the hardware and software for implementing and managing the VPN reside mainly within the premises and networks of the enterprise. The service provider may perform the actual management of the VPN, but the hardware and software reside on the enterprise site.

Service provider network-based VPNs are VPNs in which the hardware and software for implementing and managing the VPN reside in the service provider's network. Typically, the VPN hardware would be shared (in a secure fashion, of course) between multiple customers of the service provider. In addition to network-based IPsec VPNs, Multiprotocol Label Switching (MPLS) technology is emerging as an alternative VPN model for service providers. Cisco expects that, over time, MPLS-based VPNs will make up a significant portion of the service-provider VPN business. Network-based VPNs built on MPLS, however, are not appropriate for enterprise VPN deployments.

The Cisco Acquisition of Altiga Networks and Compatible Systems

Q. Why did Cisco acquire Altiga Networks?

A. On March 29, 2000, Cisco completed the acquisition of Altiga Networks to provide its customers with a market-leading, best-of-breed remote access VPN solution, including client, remote access concentrator and management products. Altiga's robust VPN solution includes a standards-based, easy-to-use VPN client, scalable VPN tunnel termination devices (also known as "VPN concentrators"), and a concentrator and client management system that enables customers to easily install, configure and manage their remote-access VPN.

Altiga's best-of-breed solutions have been recognized and validated by industry experts, as evidenced by many recently announced awards. These accolades include placement in ComputerWorld magazine's top 10 'emerging companies 2000' network and communications management category, a Network Computing Editor's Choice Award, a Mier Communications "NetWORKS As Advertised" award with recommendation as a 'good marketplace buy' and the "UUNet Tested" seal of compatibility for all Altiga VPN concentrators.

The acquisition of Altiga Networks supports the continuing enterprise VPN product strategy of Cisco and enhances its existing portfolio of VPN solutions, which includes Cisco integrated and optimized VPN routers, VPN appliances and VPN-ready cable modems and DSL solutions.

Existing Cisco VPN products include:

- The Cisco 7100 and 1700 integrated VPN routers and the Cisco 7500, 7200, 3600, 2600 and 800 Series VPN-optimized routers
- VPN appliances, including the Cisco Secure PIX firewall series, and other Cisco security appliances, such as the Cisco Secure Intrusion-Detection System and the Cisco Secure Scanner
- VPN-ready cable and DSL solutions including the Cisco 1400 DSL router and the Cisco uBR cable access router series

Q. What VPN products does Altiga Networks bring to Cisco?

A. Altiga's award-winning, best-of-breed product suite provides an integrated VPN solution for bandwidth-intensive, broadband, remote-access applications. The product suite consists of:

- VPN tunnel termination gateways (Cisco VPN 3005, 3015, 3030, 3060 Concentrators)
- VPN client (Cisco VPN Client 3000 Edition)
- VPN management and monitoring tools (Cisco VPN 3000 Monitor)

The Altiga concentrators also support Windows VPN Dial-up Networking Point-to-Point Tunneling Protocol (PPTP) and Windows 2000 (Layer 2 Tunneling Protocol [L2TP] over IPsec). The Altiga products can also be used for site-to-site VPNs, but are targeted primarily at remote access VPNs.

Public
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14807
A

Q. Didn't Cisco also acquire Compatible Systems? How do Altiga and Compatible VPN solutions compare?

A. Cisco also acquired Compatible Systems to support service provider-based VPN solutions.

While Altiga and Compatible both provide VPN products, their technologies and solutions address different applications. Altiga provides an integrated, scalable VPN solution for remote access, including client, remote access concentrator and management. Altiga's solutions are appropriate for both enterprise-managed remote access VPNs and service provider "Managed Customer Provided Equipment (CPE)" VPN services.

Compatible, on the other hand, provides a highly scalable IPsec tunnel engine as required by our service-provider customers for network-based IPsec architectures.

Q. Does Compatible provide any VPN products for the Enterprise? When would these solutions be considered for enterprise deployment?

A. The Compatible Intraport Carrier 2 and Carrier 8 VPN appliances are focused primarily on providing large-scale IPsec tunnel termination in the Internet Service Provider (ISP) environment. Some enterprises may, however, wish to deploy them within their networks.

The Compatible VPN client currently has support for Mac and UNIX desktop environments. The existing Cisco Secure VPN client and the Altiga client (to be renamed the Cisco VPN 3000 client) do not have support for Mac or UNIX environments. An enterprise customer that requires support for Mac or UNIX may consider the Compatible Intraport Carrier 2 or Carrier 8 solution for deployment.

Q. Do these acquisitions have products that will replace some Cisco products?

A. No. The Altiga VPN access concentrators fill in a specialized gap for a dedicated VPN remote-access appliance. Altiga products will complement and be used together with Cisco IOS routers and Cisco Secure PIX firewalls in remote access applications. The Altiga VPN client shares common technology with the Cisco Secure VPN client, and will serve as the basis for future VPN client releases (client road map discussed in next section.)

The Compatible Intraport Carrier 2 and Carrier 8 VPN appliances provide highly scalable IPsec tunnel termination for service-provider network VPN architectures. The Compatible products will be used together with Cisco IOS-based universal access concentrators and routers to enable VPN services to be deployed at the edge of the service-provider network regardless of access media.

Q. Both Altiga and Compatible address the VPN market. Will there be any overlap between these two companies' product lines and/or those of Cisco?

A. The product overlap is minimal and any rationalization shall evolve gradually during the integration process.

In addition to supporting service provider network VPNs, Compatible products have been used for enterprise applications. Over time, Cisco VPN architectures deployed at the enterprise premises for remote access or for site-to-site VPNs will be based on Altiga solutions and Cisco IOS VPN routers.

Cisco strategy for supporting network-based VPN solutions will be based on solutions from Compatible Solutions.

Q. Will Cisco continue development of the Cisco IOS-based VPN routers and universal access concentrators, as well as the Cisco Secure PIX firewalls for VPN applications?

A. Yes. With integrated routing, QoS, service-level validation and security features, Cisco VPN routers are the leading and preferred platforms for site-to-site VPN applications. Further, Cisco IOS-based universal access concentrators with high-performance IPsec capabilities enable service providers to deploy VPN services at the edge of their network regardless of access media.

The market-leading Cisco Secure PIX firewall offers complementary security functions for most VPN applications, providing an excellent platform for customers requiring advanced firewall capabilities.

Q. Why are these two acquisitions good for Cisco customers?

A. The acquisitions of Altiga and Compatible provide Cisco customers with:

- Integrated and scalable solution for remote access VPNs
- Highly scalable, IPsec tunnel capability in a standalone appliance. In most environments, this appliance will be deployed in service-provider networks with a Cisco IOS router or universal access concentrator.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1057
Doc. 3690

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

Altiga Product Specifics and Integration Plan

Q. How will Cisco leverage Altiga's solutions to support remote access VPNs?

A. The Cisco remote-access VPN solution, called the Cisco VPN 3000 Concentrator Series, is a best-of-breed, remote-access VPN product for enterprise-class deployment. This solution is based on the Altiga Networks product set.

The solution includes a standards-based, easy-to-use VPN client, scalable VPN tunnel termination devices, and a gateway and client management system that enables customers to easily install, configure, and manage their remote-access VPNs.

Incorporating the most-advanced, high-availability capabilities with a unique, purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator Series allows customers to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical remote-access applications. Unique to the industry, it is the only scalable platform to offer field-swappable and customer-upgradable components.

Q. Why would Cisco customers implement the Cisco VPN 3000 solution for a remote-access VPN?

A. Deploying a Cisco VPN 3000 solution for remote-access VPN enables corporations to reduce communications expenses and to leverage the existing dialup infrastructures of ISPs. At the same time, VPNs allow mobile workers and telecommuters to take advantage of broadband connectivity or local numbers to access their ISPs instead of costly long-distance or 800 numbers. As a result, corporations increase productivity and reduce expenses. To take full advantage of the unprecedented cost savings, flexibility, performance, and reliability of remote-access VPN connections, it is important to deploy a purpose-built VPN concentrator platform such as the Cisco VPN 3000 solution.

Q. What product models are included in the Cisco VPN 3000 Concentrator Series?

A. The members of the Cisco VPN 3000 Concentrator Series include the 3005, 3015, 3030 and 3060 products. This extended family of remote-access VPN concentrators supports every level of enterprise deployment, from the small branch office through the enterprise central site. Also included is the Cisco VPN 3000 client, which allows remote users to establish secure tunnels through the Internet to the Cisco VPN 3000 Concentrators. The capabilities and differences among the units are outlined in the following chart:

	Cisco 3005	Cisco 3015	Cisco 3030	Cisco 3060
Simultaneous Users	100	100	1500	5000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware
Available Expansion Slots	0	4	3	2
Encryption (SEP) Module	0	0	1	2
Redundant SEP	N/A	N/A	Option	Option
System Memory	32 MB (fixed)	64 MB	128 MB	256 MB
T1 WAN Module	Fixed option	Option	Option	Option
Hardware Configuration	1U, fixed	2U, scalable	2U, scalable	2U, scalable
Dual Power Supply	Single	Option	Option	Option
Client License	Unlimited	Unlimited	Unlimited	Unlimited

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1058
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14805
A.

Q. What are the major advantages of the Cisco VPN 3000 Concentrator Series products?

A. Some of the major advantages of the Cisco VPN 3000 Concentrator Series include:

- *Ease of Deployment and Use*—The Cisco VPN 3000 Concentrator is designed to fit into the customer's network infrastructure without requiring changes to the existing network. The Cisco VPN 3000 Concentrator will work directly with existing Remote Access Dial-In User Service (RADIUS), NT Domain or Security Dynamics (ACE) servers. This authentication versatility provides the administrator the ability to choose among the same authentication options that are available with direct dialup solutions, eliminating the need to create a second authentication database. In the absence of an existing authentication server, the Cisco VPN 3000 Concentrator has an internal authentication server that can be used for testing configurations, and can also be used to authenticate up to 100 users. The Cisco VPN 3000 Concentrator is compatible with the Cisco VPN 3000 Client, the Microsoft Windows 2000 L2TP/IPsec Client or PPTP, providing the administrator with a high degree of flexibility.
- *Performance and Scalability*—The Cisco VPN 3000 Concentrator is designed to provide the highest levels of performance in the industry. The platform supports up to 100 Mbps of sustained 3DES encrypted throughput for up to 5000 simultaneous users. Hardware-based Scalable Encryption Processors (SEPs) exist in the Cisco VPN 3030 and 3060 Concentrators to provide increased levels of encrypted throughput and numbers of simultaneous users.
- *Security*—The Cisco VPN 3000 Concentrators fully support a wide range of authentication systems, including digital certificates and tokens. In addition, the Cisco VPN 3000 Concentrators can be securely managed using HTTPS (Secure Sockets Layer [SSL]) or Secure Telnet (SSL Telnet), or through an encrypted tunnel.
- *High Availability*—The Cisco VPN 3000 Concentrator is a robust platform with a meantime between failure (MTBF) of more than 200,000 hours. Concentrators can be equipped with redundant subsystems (fans, power supplies, SEP modules) and multi-chassis fail-over (virtual router redundancy protocol [VRRP]) capabilities for maximum system uptime. The Cisco VPN 3000 Concentrator's extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early warning alerts.
- *Robust Management*—The Cisco VPN 3000 Concentrators can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, Secure Telnet, and via a console port. A consistent user interface is provided for all of these views to ease administrative training and operations requirements. Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies. In addition, the Cisco VPN 3000 Monitor provides an enterprise-wide view of the 3000 series displaying a summary of device status and vital operating statistics.
- *Ease of Upgrades*—The Cisco VPN 3000 Concentrator Series is designed to allow easy upgrades of code and hardware. This makes deployment and support faster and easier for customers. Units can be easily upgraded in the field and software can be downloaded real-time from a Web browser, from a remote location, and at a time of the administrator's choosing. This unique and flexible design can, for example, enable a Cisco customer to implement a 3015 chassis and upgrade it to the equivalent of a 3030 or 3060 as requirements increase.

Q. What VPN Protocols and routing options are supported by the Cisco VPN 3000 Concentrator Series?

A. The Cisco VPN 3000 Concentrator Series supports the following VPN protocols: IPsec, PPTP, L2TP, L2TP/IPsec, Network Address Translation (NAT) Transparent IPsec Tunneling Protocol. In addition, the following routing options are available: RIP, RIP2, OSPF, Static, Auto Endpoint Discovery, and NAT.

Q. What are the performance levels of the Cisco VPN 3000 Concentrator Series of products?

A. The performance levels of each member of the Cisco VPN 3000 Concentrator Series are included in the chart on the previous page.

Note: The Cisco VPN 3005 is a fixed-configuration, entry-level unit similar in capabilities to the 3015. However, the Cisco VPN 3015 is a scalable platform that can be upgraded to deliver performance equivalent to a 3030 or 3060.

Q. What are the latest software enhancements in the Cisco VPN 3000 Concentrator?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1059
Doc. 3690

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

A. All Cisco VPN 3000 Concentrators currently ship with Release 2.2. The following is a list of the new features provided in Release 2.1 and 2.2.

- Digital Certificates—Support for major digital certificate vendors, such as Baltimore, Entrust, Microsoft, and VeriSign
- Split Tunneling—Allows client users to access other Internet sites while securely tunneled to the Cisco VPN 3000 Concentrator
- SEP Fail-over—Improves redundancy by allowing a SEP to take over the operation and users supported by a failed SEP
- Auto Endpoint Discovery—Vastly eases VPN configuration by automatically discovering tunnel endpoints thus eliminating the need for manual tunnel configuration
- SSL (HTTPS) Support—Provides the ability to perform encrypted management to the Concentrator
- Windows 2000 Compatibility—Allows the Cisco VPN 3000 Concentrator to establish tunnels with clients using the integrated Windows 2000 L2TP/IPsec client
- IPsec/UDP support for Extranet Remote-Access VPN—Allows IPsec (Encapsulating Security Payload [ESP]) to transparently operate through a device performing NAT (port translation)

Q. What authentication mechanisms/systems does the Cisco VPN 3000 Concentrator Series support?

A. The Cisco VPN 3000 Concentrator currently supports the following authentication mechanisms/systems:

- RADIUS or RADIUS proxy
- NT Domain
- RSA Security SecurID
- X.509 Digital Certificates

Q. What are the high-availability features of the Cisco VPN 3000 Concentrator Series?

A. One of the major features of the Cisco VPN 3000 Concentrator Series is its high- availability capabilities. The concentrators are built to provide a 200,000 hour MTBF, but they also have a host of advanced capabilities to protect against failure within units as well as among units.

The Cisco VPN 3000 Concentrator Series all support redundancy options, including dual-redundant and hot- swappable power supplies. Power supply statistics are kept in the unit and are available through various management methods such as HTML and provide temperature, fan speed and status information. Change in status causes alarms, which in turn allow operators to swap power supplies without affecting customer operation.

The Cisco VPN 3000 Concentrators support optional redundant SEPs. In the event of a single SEP failure, a backup SEP will take over the existing sessions with no effect on the active users. Users remain unaware of the change. In the unlikely event that the backup SEP then fails or that no backup SEP exists, the unit reverts to software encryption. Throughput would be limited to the maximum available in software (4 Mbps), but sessions would remain intact.

In addition, the Concentrators themselves are equipped with a fail-over mechanism using the VRRP that allows for a backup hot-standby unit to be available in case of system maintenance or failure. Each is designated as the slave to the other and should a unit fail completely, the other unit will recognize the failure and take over the operation of the sessions. These features are designed to ensure that the Cisco VPN 3000 Concentrator is never unreachable.

Q. Where would you deploy the Cisco VPN 3000 Concentrator in the network?

A. The Cisco VPN 3000 Concentrators can be deployed in multiple locations within a customer network. Typically, a Cisco VPN 3000 Concentrator will be implemented to support remote-access VPNs. In this application, the Cisco VPN 3000 Concentrator will be deployed behind a customer's Internet router and either in parallel to or behind a customer's firewall (depending upon business requirements and security policy).

Q. Does the Cisco VPN 3000 Concentrator Series have an integrated firewall? If so, what features are supported?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1060
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14.803
A.

A. Yes, the Cisco VPN 3000 Concentrator has an integrated firewall. This firewall provides stateless packet filtering and NAT. (Note: The integrated firewalling capability within the Cisco VPN Concentrator 3000 series is not intended to replace a fully featured firewall, such as the Cisco Secure PIX Firewall.)

Q. To what countries can Cisco export the Cisco VPN 3000 Concentrator Series?

A. Cisco can export the Cisco VPN 3000 Concentrator Series to all countries except those in the "T7" countries, including Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. The T7 countries have been identified by the U.S. government for involvement in terrorist activities, and the export of encryption products to these countries is prohibited.

Other countries may also have restrictions on importing encryption products. Each country operates differently and its government should be consulted prior to import of the Cisco VPN 3000 Concentrator solution.

The official Cisco export policy can be found at http://www.cisco.com/ww1/export/crypto/tool.

Q. What encryption algorithms are supported in the Cisco VPN 3000 Concentrator Series?

A. The Cisco VPN 3000 Concentrator Series supports DES, 3DES, and RC4 encryption standards. DES and 3DES are typically used with the IPsec protocol suite, and RC4 is used with the PPTP protocol.

Q. Can the Cisco VPN 3000 Concentrator Series terminate tunnels initiated from Windows clients?

A. Yes, the Cisco VPN 3000 Concentrator Series can terminate PPTP tunnels initiated from Windows 95/98/NT/2000 clients.

For Windows 2000 support, the Cisco VPN 3000 Concentrator Series also supports the native L2TP/IPsec client that ships with Windows 2000. (Note: To use the Windows 2000 native L2TP over IPsec client, digital certificates must be used for the IKE—phase I authentication. Windows 2000 Advanced Server ships with a native Certificate Authority (CA), and either the Microsoft native CA or those from third-party vendors may be used. User-based (phase II) authentication can still take place in the usual manner using NT or RADIUS authentication.)

Q. What WAN support is available in the Cisco VPN 3000 Concentrator Series?

A. Initially, the Cisco VPN 3000 Concentrator Series provides T1 support. E1 support is planned for a future release.

Q. What is the new Cisco VPN 3005 Concentrator model?

A. The Cisco VPN 3005 is a fixed-configuration, lower-priced VPN Concentrator model for customers who do not anticipate the need to upgrade for greater performance. It is ideal for small offices requiring a smaller number of remote-access sessions and for service providers that wish to offer customer provided equipment (CPE)-based managed services.

Q. How does the VPN 3005 Concentrator compare to the VPN 3015 Concentrator?

A. The Cisco VPN 3005 generates the same performance and supports the same number of users as the 3015. Also, as in the 3015, the 3005 includes unlimited client licenses at no extra cost.

There are, however, a number of differences between the two models. Notably, the list price of the Cisco VPN 3005 is 40 percent less than that of the 3015. Both models are rack mountable, but the 3005 chassis is half the size (1U) of the 3015 chassis (2U). Unlike the 3015, the power supply in the 3005 is not field-replaceable and the 3005 cannot be upgraded to hardware encryption.

Q. Is the new Cisco VPN 3005 Concentrator upgradable?

A. No, the Cisco VPN 3000 Concentrator is offered in a fixed configuration only. The 3005 platform is designed to provide robust remote-access VPN capabilities at a lower cost and serve the needs of the small/remote office and CPE-based managed services markets.

Q. What is the difference in WAN support between the VPN 3005 Concentrator and the other VPN Concentrator models?

A. If customers require WAN support with the 3005, they must order the unit with a WAN module installed. All other models in the Cisco VPN 3000 Concentrator Series are field-upgradable, enabling customers to add a WAN module at any time.

Q. Is redundancy available in the VPN 3005 Concentrator?

A. VRRP and redundant fans are included to provide high availability. However, there are no other redundant subsystems in the 3005.

ROS nº 03/2005 - CN
CPMI - CORREIOS
1061
Fls. Nº
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14.802

Q. Can the Cisco VPN 3000 Client V2.2 be installed via floppy disks?

A. Yes. Administrators can create a Cisco VPN 3000 Client V2.2 installation floppy disk set for deployment to their desktops.

Q. What are the parameters that need to be configured in the Cisco VPN 3000 Client V2.2 itself (as opposed to those configured in the Concentrators)?

A. The only parameters that need to be configured within the Cisco VPN 3000 Client V2.2 are the destination concentrator's IP address or DNS name and either 1) the VPN user group and password or 2) the digital certificate authority to be used. The remote user will always be prompted for a username and password for network access authentication.

Q. Can the Cisco VPN 3000 Client V2.2 be deployed with all parameters pre-configured?

A. Yes. Administrators can create a Cisco VPN 3000 Client V2.2 installation that includes all client-configuration parameters preset so that the installation is completely hands-free for end users. Information regarding creation of a predefined configuration is noted in the documentation.

Q. Which operating systems does the Cisco VPN 3000 Client V2.2 support?

A. The Cisco VPN 3000 Client V2.2 will run on Win9X and WinNT. The Cisco VPN 3000 Client V2.2 does not currently run on Windows 2000. Support for Windows 2000 will be available in a future release.

Q. Does all remote access VPN traffic have to go through an encrypted tunnel to the concentrator at the enterprise or service provider? (for example, can plain Web access to other sites go in the open, directly out through the ISP's Internet connection?)

A. Yes. This concept is known as "split tunneling." Split tunneling allows for secure access to corporate resources via an encrypted tunnel while allowing Internet access directly through the ISP's resources (eliminating the corporate network from the path for Web access). Cisco VPN 3000 Concentrator series and the Cisco VPN 3000 Client V2.2 can support split tunneling. For additional security, this feature is controllable by the administrator of the concentrator and not the user.

Q. Can the Cisco VPN 3000 Client V2.2 support extranet remote-access VPN deployments? In other words, does the Cisco VPN 3000 Client V2.2 work behind devices performing Network Address Translation?

A. In general, IPsec (ESP) can work behind devices performing NAT. However, most devices that do NAT (port address translation), do not yet understand ESP (only transmission control protocol [TCP], user diagram protocol [UDP], Internet control message protocol [ICMP]). For this reason, the Cisco VPN 3000 Client V2.2 provides a NAT-transparent IPsec (ESP) option, which is configurable per user group in the Cisco VPN 3000 Concentrator. This option enables Cisco customers to support extranet remote-access VPNs.

Q. Does the Cisco VPN 3000 client support data compression?

A. At this time, the Cisco VPN 3000 client does not support compression. However, support for data compression is planned in a future release.

Q. Does the Cisco VPN 3000 client have any firewall options or functionality?

A. At the present time, the Cisco VPN 3000 client has no integrated firewall functionality. Note, however, while an IPsec tunnel is up and running, no packets other than those from the secure corporate network will be allowed to enter the client machine unless "split tunneling" is being used as described previously.

Q. Does the Cisco VPN 3000 client offer "failover" features?

A. Yes, the Cisco VPN 3000 client provides a "failover" feature for multiple Concentrator destinations.

Q. What are the advantages of using the Cisco VPN 3000 Client V2.2 over an operating system-native VPN client such as those offered by Microsoft?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1062
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14.801
A.

A. The Cisco VPN 3000 Client offers a tight integration between concentrator and client and allows for centralized policy control as well as a richer feature set (such as split tunneling and IPsec/UDP). With a Cisco VPN 3000 solution, an administrator can easily define client policies, which are stored on a Cisco VPN 3000 Concentrator. When a remote user running a Cisco VPN 3000 Client attempts to connect to a Cisco VPN 3000 Concentrator, the Concentrator provisions the defined policy to the client. This design provides a tightly integrated, easily managed solution and enables rapid deployment of remote-access VPNs.

The native VPN client in Windows 2000 requires digital certificates for the first phase of authentication and does not provide the additional value-added features of the Cisco VPN 3000 client described above. However, for some customers, the ability to have an integrated client may be more important. The Cisco VPN 3000 Concentrator is one of the only VPN solutions in the market that provides a choice for remote client software.

Q. What is the per-user license cost of the Cisco VPN 3000 client V2.2?
A. The Cisco VPN 3000 client V2.2 is included at no cost with all Cisco VPN 3000 Concentrators models and includes licensing for an unlimited number of clients for use with the purchased VPN 3000 Concentrator.

Q. Will the Cisco VPN 3000 client interoperate with Cisco IOS routers and Cisco Secure PIX firewalls?
A. Initially, the Cisco VPN 3000 client will not interoperate with Cisco IOS routers or Cisco PIX firewalls. In a future release, the Cisco VPN 3000 client will interoperate with both Cisco IOS routers and Cisco Secure PIX firewalls.

Q. Will Cisco continue to ship the Cisco Secure VPN client? If so, why?
A. Yes, Cisco will continue to ship the Cisco Secure VPN client until the Cisco 3000 VPN client is interoperable with Cisco IOS routers and Cisco Secure PIX firewalls. The Cisco Secure VPN client currently interoperates only with the Cisco IOS routers and Cisco Secure PIX firewalls.

Q. Will Cisco also ship the client provided with the Compatible Systems-based VPN solution?
A. Yes, Cisco will also ship the client provided with the Compatible-Systems-based VPN solution. This particular client interoperates with only the Compatible Systems-based devices. It does not interoperate with Cisco IOS routers, Cisco Secure PIX firewalls, or Cisco VPN 3000 Concentrators.

Q. If a customer absolutely requires VPN client support on Mac or UNIX platforms, which Cisco solution should the customer use?
A. If a customer requires Mac/UNIX-based platform support, the customer should implement the Compatible Systems-based VPN solution.

Q. What is the Cisco client strategy?
A. As described above, Cisco intends to continue to ship multiple clients in the near future. The Cisco VPN 3000 client will be modified in a future release to interoperate with Cisco IOS routers and Cisco Secure PIX firewalls. Ultimately, Cisco plans to migrate to a unified client that integrates with Cisco VPN 3000 Concentrators, Cisco IOS routers, Cisco Secure PIX firewalls, and compatible Systems-based devices. By implementing this strategy, Cisco will be able to provide a single user interface and feature set across the entire spectrum of enterprise and service provider customers.

Cisco also plans to continue working with the major operating systems vendors, such as Microsoft, as they continue to incorporate and enhance the IPsec client support in their products.

Q. How does an administrator manage the Cisco VPN 3000 Concentrator Series?
A. The Cisco VPN 3000 Concentrator Series employs multiple methods of management including Console (ASCII terminal) for local connections, Telnet and Secure Telnet, and HTTP browser access. The management channel can be secured to protect management data from being visible by a packet sniffer. Customers can access any unit via the embedded Web manager and view status or change configuration. There is a high degree of flexibility in how operators can be secured as well by allowing scalable supervisor privileges. This technique makes the Cisco VPN 3000 Concentrator among the easiest to manage while providing a robust management feature set.

Q. Does the Cisco VPN 3000 solution provide Management Information Bases (MIBs)?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1063
Doc. 3690

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14.800

A. Yes, the Cisco VPN 3000 solution provides a high-level IPsec MIB and L2TP/PPTP MIBs. In addition, the 3000 Concentrators support MIB2 and an enterprise MIB providing vital device statistics.

Q. Does the Cisco VPN 3000 solution provide MIBs?

A. Yes, the Cisco VPN 3000 solution provides a high-level IPsec MIB as well as MIB2, and L2TP/PPP MIBs.

Q. What event information is supported in the Cisco VPN 3000 solution?

A. The Cisco VPN 3000 solution provides simple network management protocol (SNMP) traps, syslog, and e-mail notifications.

Q. What is the Cisco VPN 3000 Monitor application?

A. The Cisco VPN 3000 Monitor application is an enterprise-wide monitoring application that allows IT personnel the ability to monitor the status and health of the Cisco VPN 3000 Concentrators. It provides easy-to-view status information such as device availability, active sessions, throughput, and central processing unit (CPU) utilization on multiple colocated VPN 3000 Concentrators. The Cisco VPN 3000 Monitor application is easy to navigate and operates on Windows 95, 98, NT and 2000.

Q. What VPN platforms does the Cisco VPN 3000 Monitor application support?

A. The Cisco VPN Monitor application will only support the Cisco VPN 3000 Concentrator series and Cisco VPN 3000 client. Currently, the Cisco VPN 3000 Monitor is compatible with the 3015, 3030, and 3060 models of the Cisco VPN 3000 Concentrator Series.

Q. How will Cisco manage IPsec VPNs on Cisco IOS routers and Cisco Secure PIX firewalls (in other words, how will Cisco support site-to-site and firewall-based VPN environments?)

A. Cisco will manage the IPsec VPN configurations between Cisco IOS routers and Cisco Secure PIX firewalls with the Cisco Secure Policy Manager V2.0. CSPM can enable an administrator to define, distribute, and enforce security and VPN policy in a site-to-site environment.

Site-to-site VPNs are an extension of the classic WAN. In this regard, additional VPN management issues should be considered in a site-to-site VPN, including quality of service and service-level management. These functions are addressed within the CiscoWorks 2000 suite of management solutions.

Q. How does Cisco plan to integrate the management of Cisco VPN clients and gateways?

A. Cisco will migrate the VPN management solutions into a unified management environment by:

1. Providing an embedded, Web-based management solution for all Cisco VPN platforms, including Cisco VPN 3000 Concentrators, Cisco IOS routers, and Cisco Secure PIX firewalls. Each of these devices will utilize an intuitive management interface with a common look and feel to ensure ease of use and reduced learning/training time.
2. Delivering a comprehensive multi-device, network-wide VPN management system for remote-access, site-to-site, and firewall-based VPNs. This system will be based in the CiscoWorks 2000 framework and will provide network-wide configuration and monitoring of Cisco VPN 3000 Concentrators, Cisco IOS routers, and Cisco Secure PIX firewalls.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

ROS nº 03/2005 - CN
CPMI - CORREIOS
1064
Fls. Nº
3690
Doc.

14.799 A.

Additional New Product Information

Cisco Secure PIX Firewall 506

Q. What type of firewall is the Cisco Secure PIX firewall 506? How is the PIX 506 different from other firewall products on the market?

A. The PIX firewall 506 is part of the Cisco Secure PIX Firewall Series of standalone, special-purpose firewalls that deliver stateful security and extremely fast performance. PIX firewalls thoroughly conceal an internal network from the outside world—providing full firewall security protection. Unlike typical CPU-intensive proxy servers running on general-purpose operating systems that perform extensive processing on each data packet, PIX firewalls use stateful analysis technology implemented in a secure, real-time, embedded operating system. This approach enables The Cisco Secure PIX firewall series to deliver outstanding performance, dramatically surpassing the performance of general-purpose, operating system-based firewalls.

Q. What is the difference between the new Cisco Secure PIX firewall 506 and the other Cisco Secure PIX firewall platforms?

A. The Cisco Secure PIX Firewall 506 delivers enterprise-class security, performance and VPN capabilities in a very small chassis at very low cost. The PIX 506 is designed for small businesses and small branch offices. The PIX 515 is a slim-line, Ethernet-only PIX hardware platform designed for small-to-medium locations, including enterprise branch/regional offices. The PIX 520 is an enterprise-class chassis with greater processor power, a larger number of interface options, and support for higher volumes of traffic than any firewall device in the world. All Cisco Secure PIX firewall platforms provide industry-leading performance, security, and reliability.

Q. What are the specifications for the Cisco Secure PIX firewall 506?

A. The Cisco Secure PIX firewall 506 has 32 MB RAM, 8 MB Flash, 200 MHz Pentium III processor, and two integrated 10BaseT Ethernet interfaces

Q. What type of performance can I expect with the PIX 506?

A. The PIX 506 efficiently handles throughput of 10 Mbps and 3DES encryption at 4 Mbps.

Q. Does the Cisco Secure PIX firewall 506 support fail-over?

A. The PIX 506 does not support fail-over mode. Most Cisco Secure PIX firewall 520 and 515 models can be run in fail-over mode with a second PIX firewall.

Q. What is the primary Cisco Secure PIX firewall application?

A. The PIX 506 specifically targets the small-business and small-branch office markets.

Q. How secure is the Cisco Secure PIX firewall 506?

A. The Cisco Secure PIX firewall 506 is built from the same operating system and technology found in the PIX 520, which the U.S. National Security Agency-sponsored Trusted Technology Assessment Program (TTAP) recently awarded its highest security rating any commercial firewall product (http://www.cisco.com/warp/customer/779/gov/federal/TTAP/).

Q. Do you need additional hardware platforms to run the Cisco Secure PIX firewall 506?

A. No. The Cisco Secure PIX firewall itself is a turnkey hardware solution—a network appliance with embedded software, so no additional platforms are required.

Q. Are there any special environmental considerations for Cisco Secure PIX firewall 506 deployment?

A. No. The Cisco Secure PIX firewall operates in environments where 110-240 VAC is available, and supports a frequency of 50-60 Hz.

Q. Can I rack-mount the Cisco Secure PIX firewall 506?

A. No. The PIX firewall 506 was designed to be a freestanding unit.

Q. Can I add network interfaces to the Cisco Secure PIX firewall 506?

A. No. The PIX firewall 506 only supports the two integrated 10BaseT Ethernet interfaces.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
3590
Doc.

Public
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

14.798
A.

Q. Does the Cisco Secure PIX Firewall support IPsec VPN tunnels?

A. Yes. The PIX Firewall 506 supports IPsec-based VPNs. The PIX firewall implementation of IPsec is based on the Cisco IOS IPsec implementation and provides seamless functionality with those IPsec-compliant products that already work with Cisco IOS IPsec, such as the Cisco Secure VPN client.

Q. How would a Cisco Secure PIX firewall 506 be deployed in a VPN environment?

A. The PIX firewall 506 would be deployed primarily in a site-to-site topology, where the PIX firewall 506 in a remote location would securely connect and transmit information to a central site VPN device, such as a Cisco IOS router or PIX 520 or 515 firewall.

Q. When will the Cisco Secure PIX firewall 506 be available?

A. Cisco expects to begin shipping the Cisco Secure PIX Firewall 506 in the second quarter of 2000.

Cisco Secure Policy Manager V2.0

Q. What is Cisco Secure Policy Manager?

A. Cisco Secure Policy Manager (CSPM), formerly known as Cisco Security Manager, is a policy-based security management system for Cisco firewalls and IPsec VPN gateways. Cisco Secure Policy Manager enables an administrator to define, enforce and audit security policies for distributed Cisco Secure PIX firewalls and VPN gateways as well as Cisco routers running the Cisco Secure integrated software and Cisco Secure integrated VPN software feature sets.

CSPM provides a scalable, comprehensive security management system for Cisco security devices. The product's intelligent, policy-based management approach enables an administrator to define intuitive, business-level directives to control access to network resources. CSPM translates these policies into the required configuration commands, distributes them to the appropriate network devices, and enforces security policy as required. The product also provides administrators with basic auditing and reporting mechanisms for event and log analysis.

Q. What are the key features and benefits of Cisco Secure Policy Manager 2.0?

A. The main features of CSPM 2.0 and benefits are as follows:

- *Cisco Firewall Management*—Easily defines perimeter security policies for Cisco Secure PIX Firewalls and Cisco routers running the Cisco Secure integrated software feature set
- *Cisco VPN Gateway Management*—Easily configures intranet/extranet IPsec VPNs based on Cisco Secure PIX firewalls and Cisco routers running the Cisco Secure integrated VPN software feature set
- *Security Policy Management*—Uses network-wide policies to manage up to several hundred Cisco security devices without requiring extensive device knowledge and dependency on the command-line interface (CLI)
- *Intelligent Network Management*—Translates defined policies into the appropriate device commands and then securely distributes these configurations throughout the network to reduce the requirement for device-by-device management
- *Notification and Reporting System*—Provides basic auditing tools to monitor, alert, and report Cisco security device and policy activity, to keep the network administrator readily informed of network-wide events
- *Windows NT-based System*—Provided in an easy-to-use Windows-based user interface

Q. What devices can Cisco Secure Policy Manager 2.0 administer within a network?

A. Cisco Secure Policy Manager V2.0 provides policy-based administration of Cisco Secure PIX firewalls as well as Cisco routers and VPN gateways running the Cisco Secure integrated software and Cisco Secure integrated VPN software features. More specifically, CSPM V2.0 supports the following devices and software versions:

- Cisco Secure PIX firewalls: 515 and 520 models running PIX OS 4.2.4, 4.2.5, 4.4.x and 5.1.x.

Note: PIX OS 5.0.x is not supported in CSPM.

nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1066
Doc 3690

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

• Cisco routers: 1720, 2600, 3620, 3640, 7100 and 7200 running Cisco IOS software Versions 12.0(5)T, 12.0(7)T, 12.0(5)XE5

Q. Who should use Cisco Secure Policy Manager 2.0?

A. Cisco Secure Policy Manager 2.0 is an appropriate management solution for any enterprise-class or small-business network environment containing Cisco firewalls and/or Cisco VPN gateways.

Q. How many devices can Cisco Secure Policy Manager administer?

A. Cisco Secure Policy Manager 2.0 can effectively manage several hundred Cisco firewalls and VPN gateways. While the product has been tested with up to 500 devices, the exact number of supported devices depends on the following points:

- The number of managed devices
- The number of interfaces per device
- The complexity of network topology (for example, meshed vs. hub-and-spoke)
- The size and complexity of network policies and configurations
- The power of the host system running the CSPM application.

Q. What future enhancements are planned for Cisco Secure Policy Manager?

A. Future versions of CSPM will provide enhancements to support additional Cisco security technologies such as intrusion-detection services and user-based security policies. Additionally, integration with CiscoWorks2000 is planned for later in CY2000.

Q. Can I use Cisco Secure Policy Manager to configure my existing Cisco IOS routers and Cisco Secure PIX firewalls in my network?

A. Yes, CSPM enables a network administrator to manage existing Cisco security devices throughout the network. The existing Cisco devices within the network must be manually added to the CSPM system prior to defining and distributing policies to them. Using CSPM's built-in "wizards" simplifies and expedites this process.

Q. Can Cisco Secure Policy Manager configure new Cisco firewalls and Cisco IOS routers within my network?

A. Yes, CSPM enables a network administrator to configure newly installed Cisco firewalls—including Cisco Secure PIX firewalls and Cisco IOS firewalls—and VPN support in both Cisco Secure PIX firewalls and Cisco IOS routers throughout the network. The product is most appropriate in environments where new Cisco security devices are being deployed.

Q. Does Cisco Secure Policy Manager offer any reporting capabilities on the security status of my network?

A. Yes, CSPM provides Web-based reports in graph and text format on the status of security policies and events within the network. These reports are quite basic and are based upon filtered syslog messages received from the managed devices.

Q. Does Cisco Secure Policy Manager provide any alarms or alerts for abnormal security events within my network?

A. Yes, CSPM provides an event-notification system for monitoring and logging Cisco firewall and VPN gateway events originating from within the managed network. This event- notification system is based on tracking and filtering syslog messages. The network administrator can define specific event filters and thresholds as well as the action that must be taken as a result of the event (for example, logging, e-mail alert, audible alert, and executing a script).

Q. Does Cisco Secure Policy Manager provide any alarms or alerts for abnormal security events within my network?

A. Yes, CSPM provides an event notification system for monitoring and logging Cisco firewall and VPN gateway events originating from within the managed network. This event-notification system is based on tracking and filtering syslog messages. The network administrator can define specific event filters and thresholds as well as the action that must be taken as a result of the event (for example, logging, e-mail alert, audible alert, and executing a script).

Q. On what operating systems does Cisco Secure Policy Manager run?

A. CSPM 2.0 runs on Windows-based systems. The product can be installed in several modes, which will dictate which operating systems are supported.

Q. Does Cisco Secure Policy Manager offer any Web browser-based applications?

A. Yes, CSPM provides Web-browser-based reports that are accessible from authorized clients running these Internet browsers:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1067
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

1479
A.

- Microsoft Internet Explorer 5.0
- Netscape Navigator 4.x

Q. Does Cisco Secure Policy Manager use a Web server for its Web-based reports? If so, which one?
A. Yes, CSPM uses a Web server to provide its Web-based reports on security policy and status. The Web server that is embedded in the policy server is from Apache and does not require a separate installation process.

Q. Can I use my existing Microsoft or Netscape Web server to run the reports within Cisco Secure Policy Manager?
A. No, the Web-based reports within Cisco Secure Policy Manager are currently only supported by the Web server embedded within the policy management system.

Q. Does Cisco Secure Policy Manager use a database?
A. Yes, CSPM uses a proprietary object-oriented database that has been optimized and secured for use in the policy-based management system. The object schema employed within this database is consistent with the work being done within the Directory Enabled Networks (DEN) initiative.

Q. Does Cisco Secure Policy Manager integrate with any directory services?
A. No, Cisco Secure Policy Manager does not currently integrate with any network directories. However, future product releases will support network directories to provide enhanced policy management.

Q. Does Cisco Secure Policy Manager integrate with CiscoSecure access control servers?
A. No, Cisco Secure Policy Manager 2.0 does not integrate with CiscoSecure access control server (ACS). However, Security Manager does allow a network security administrator to configure managed Cisco devices to interoperate with CiscoSecure ACS. Through simple command line-based configurations, CSPM can configure selected Cisco routers and firewalls to access CiscoSecure servers for the appropriate authentication, authorization, and accounting (AAA) services.

Q. Does Cisco Secure Policy Manager integrate with any certificate authority servers?
A. Yes, Cisco Secure Policy Manager 2.0 provides very basic support for CA servers within a VPN network. CA servers can be added to the network topology so Cisco devices can identify and communicate with them to acquire a certificate for authentication purposes. Certificate information such as owner, signing authority, serial number, and supported time frame can be discovered for each supported device. CSPM provides support for CA servers by Entrust and VeriSign.

Cisco 1700 Router VPN Module

Q. What is the Cisco 1700 series?
A. The Cisco 1700 series, which includes the Cisco 1720 and 1750 models, is a New World service, modular-access router for small- and medium-sized businesses and small branch offices. It delivers a rich, integrated package of routing, firewall, and VPN functions for Internet data and voice applications. The Cisco 1700 series, together with the VPN module and Cisco Secure integrated software (formerly the Cisco IOS Firewall Feature Set), is the perfect IPsec-VPN solution for connecting small offices to other remote offices, mobile users, central-office intranets, or partner extranets.

Q. What is the new 1700 VPN module and what does it do?
A. The VPN module for Cisco 1700 series routers optimizes the platform for IPsec VPNs. The module not only accelerates the 3DES and DES encryption algorithms used in IPsec, but also handles a variety of other IPsec-related tasks—hashing, key exchange, and storage of security associations. By doing so, the module frees the Cisco 1700 main processor and memory to perform other router, voice, and firewall functions.

Q. What is the performance of the 1700 VPN module?
A. The VPN module accelerates IPsec (3DES) at speeds suitable up to a full-duplex T1/E1 (4 Mbps for 1514-byte packets). The module, together with the platform, supports as many as 100 encrypted tunnels for concurrent sessions with mobile users or other sites.

Q. What are the key features of the 1700 VPN module?
A. The key features of the 1700 VPN module include the ability to:

RQS nº 03/2005 - CN
CPML - CORREIOS
Fls. Nº 1068
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

JU 795
A-

- Accelerate IPsec at speeds suitable up to a full-duplex T1/E1 (3DES, 4 Mbps, 1514-byte packets)
- Deliver up to 100 concurrent sessions (IPsec tunnels)
- Implement 3DES or DES for data protection
- Support RSA Signatures and Diffie Hellman for authentication
- Use SHA-1 or MD5 hashing algorithms for data integrity

Q. How does the Cisco 1700 with VPN module compare to Cisco 1700 with IPsec software alone? How about the Cisco 1600 and Cisco 800?

A. The Cisco 1700 with IPsec software and no VPN module can achieve 300 Kbps with 256-byte packets (3DES). With the VPN module, the Cisco 1700 can deliver 3400 Kbps with the same packet sizes. The Cisco 1600 and Cisco 800 support DES encryption only (not 3DES) and reach speeds suitable for ISDN connections (128 Kbps).

Q. How does the Cisco 1700 with the VPN module fit within the product line of Altiga?

A. The Cisco 1700 Series with the VPN module is a world-class router that delivers world-class WAN connectivity, voice, firewall protection, and IPsec tunnel serving. The Cisco 1700 Series may be deployed for VPNs for both site-to-site and limited remote-access (such as for connecting mobile users and telecommuters) applications. The Altiga solution provides a state-of-the-art VPN concentrator, VPN client and management system designed specifically for remote access, but it has limited routing, firewall, and WAN capabilities. The Altiga solution is particularly suited for adding remote-access VPNs to legacy networks. The Cisco 1700 Series is best for the small-office environment, where integration is valued over a multiple box solution.

Q. Does the Cisco 1700 with VPN module interoperate with IPsec VPN solutions from other vendors?

A. Though vendors are converging on the IPsec standard as well as standards for Public Key Infrastructure and digital certificates, many have implementations that contain proprietary features. As a consequence, interoperability may be limited. However, Cisco was instrumental in the development of IPsec, and continues to work with other industry participants to evolve the standard and improve vendor interoperability.

Q. What management tools are available that support configuration and monitoring of the Cisco 1700 Series with VPN module?

A. For management of firewall and VPN features on the Cisco 1700 Series routers, Cisco ConfigMaker provides an easy-to-use graphical user interface (GUI) suitable for basic configuration and monitoring. Cisco Secure Policy Manager is a comprehensive management tool for large-scale deployments. The Cisco 1700 Series routers with VPN module are also supported in CiscoWorks2000 CiscoView.

Q. Is the VPN module supported on all Cisco 1700 models?

A. Yes. The VPN module is supported on the Cisco 1720 and Cisco 1750, Cisco 1750-2V, and Cisco 1750-4V.

Q. How is the VPN module installed?

A. The VPN module fits in the expansion slot inside the chassis. Although the module itself can be used in any Cisco 1700 model, the Cisco 1720 requires a different retention clip than the Cisco 1750 does. (See "Installing the Cisco 1700 Series Encryption Module.")

Q. Does the VPN module support IP compression?

A. When the VPN module is enabled, IP compression is disabled on the Cisco 1700 Series. IP compression is touted by some vendors, but the benefits are typically negligible for the small-branch office environment.

IPsec adds 42 bytes to the length of any IP packet. This addition results in fragmentation for packets originally near the maximum (1514 bytes). The module for the Cisco 1700 Series encrypts large packets so quickly, the process time of a large packet and fragment is negligibly longer than the process time of one compressed large packet. In other words, for the Cisco 1700 routers themselves, compression is not expected to provide great benefits. Customers have the option of eliminating fragmentation by reducing the maximum packet size to about 1472 bytes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1069
3690
Doc.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

When the VPN module is disabled, IP compression and IPsec operations may be performed using the IPsec software and main processor, but overall performance will degrade (300 Kbps with 256-byte packets).

Q. Does the Cisco 1750 with VPN module support both IPsec and Voice over IP?

A. The Cisco 1750 with VPN module can support data traffic over an IPsec tunnel and simultaneously convey voice traffic using standard IP. Voice traffic over an IPsec tunnel on the Cisco 1750 is not supported on initial release—Cisco IOS 12.1(1)XX—but is planned for a future release.

Q. Does the VPN module support process switching, fast switching, and Cisco express forwarding (CEF)?

A. The VPN module does support process switching and fast switching, but it does not currently support CEF.

Q. What software options are available for the VPN module?

A. The VPN module is supported on releases 12.1(1)XX, 12.1(2)T and later of the Cisco 1700 Series IOS software. IPsec 3DES software contains all the IPsec features of Cisco 1700 Series IOS software and supports both 3DES and DES (56-bit). IPsec 56 software includes the same set of IPsec features, but only supports DES (56-bit). For example, Cisco 1700 Series IOS IP Firewall Plus IPsec 3DES software for 12.1(2)T includes the full IPsec package, 3DES and DES, firewall, and plus features.

A Cisco 1700 Series router with a VPN module installed will run with any feature set for the Cisco 1700 Series IOS software (12.1(1)XL, 12.1(2)T and later), but the module is only used with IPsec feature sets. For example, Cisco 1700 Series IOS IP only software for 12.1(2)T will run on a Cisco 1700 Series router with the VPN module installed, but it will not be enabled for IPsec and will not exploit the features of the VPN module.

Additional New Product Information

Q. Where can I find additional information on the Cisco VPN strategy and products?

A. For more information, review the Cisco VPN Web site at http://www.cisco.com/go/evpn/.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1070
Doc. 3690

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Connection Online Web site at http://www.cisco.com/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000 Cisco Systems, Inc. All rights reserved. Printed in the USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. PIX is a trademark. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9912R)

04/00 RW6049

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

NEC DO BRASIL S/A – MANUAL VOLUME IV

2003
PASTA 26

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1071
Doc. 3690

E C T
1613
CPL - AC

Intrusão doc 1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1072
Doc: 3690

Cisco Systems

Data Sheet

Cisco **IDS 4200** Series Sensors

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs.

The Cisco IDS 4200 Series sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Additionally, Cisco's flexible deployment options allow businesses to minimize the total cost of ownership of their IDS deployments by delivering:

- unprecedented price/performance ratios
- the ability to simultaneously protect multiple network subnets through the support for multiple sniffing interfaces, thereby delivering up to five sensors in one
- a wide array of performance options
- investment protection by delivering modular, upgradable components
- support for multi-VLAN traffic
- embedded web-based management solutions packaged with the IDS sensors

Please refer to Table 1 for information on the characteristics of the Cisco IDS 4200 Series Sensors.

For details on the complete Cisco Intrusion Protection System, go to http://www.cisco.com/go/ids.

Deploying the Cisco IDS 4200 Series Sensors

The Cisco IDS 4200 Series includes four products: the Cisco IDS 4215, IDS 4235, IDS 4250 and IDS 4250-XL sensors. The Cisco IDS product line delivers a broad range of solutions that allow easy integration into many different environments, including enterprise and service provider environments. Each sensor addresses the bandwidth requirements at one of several speeds, from 80 Mbps to gigabits per second.

The Cisco IDS 4215 can monitor up to 80 Mbps of traffic and is suitable for T1/E1 and T3 environments. Additionally, multiple sniffing interfaces are supported on the IDS-4215 which allow the ability to simultaneously protect multiple subnets, thereby delivering five sensors in a single unit.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces it can also be deployed on partially utilized gigabit links.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1073
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

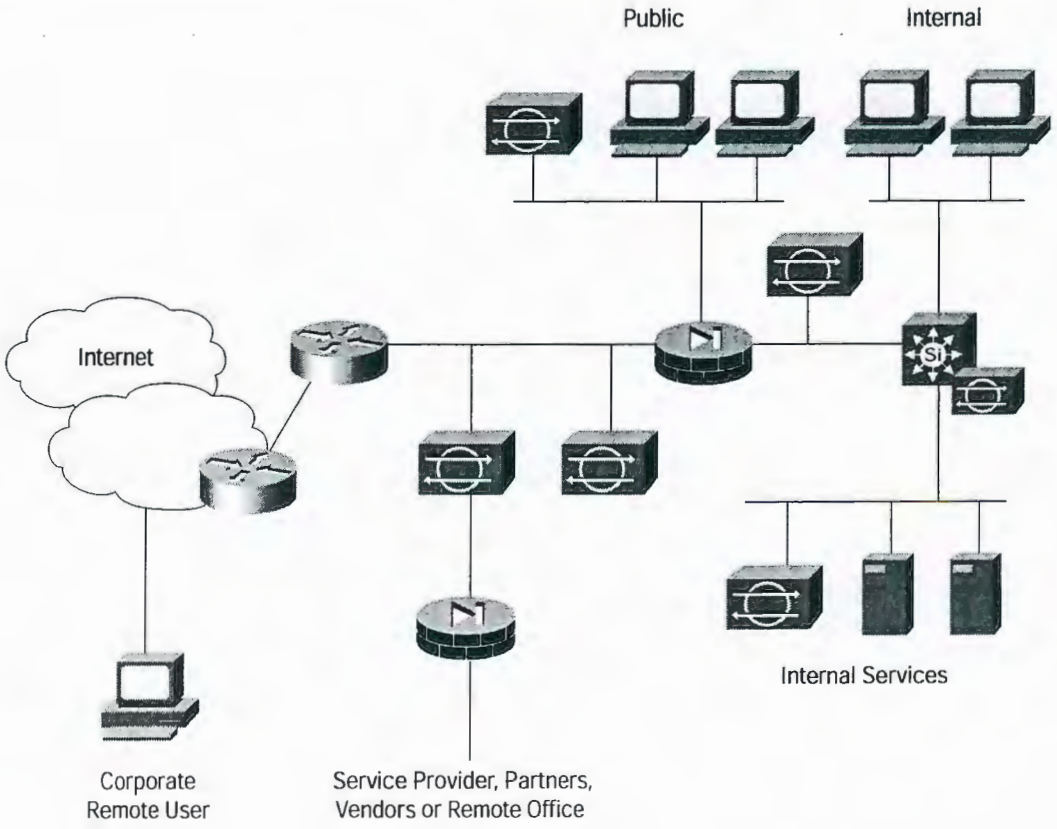
The Cisco IDS 4250 supports a 500 Mbps speed and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets. In addition, the Cisco IDS 4250 provides the flexibility to accommodate a simple hardware upgrade to scale to full line-rate gigabit performance.

At 1 Gbps, the Cisco IDS 4250-XL provides unprecedented performance by providing customized hardware acceleration to protect fully-saturated gigabit links as well as multiple partially-utilized gigabit subnets.

As shown in Figure 1, sensors can be placed on almost any network segment of the enterprise-wide network where security visibility is required.

Please refer to Table 2 for ordering information for the Cisco IDS 4200 Series Sensors.

Figure 1
Deployment Scenarios for the 4200 Series Appliance Sensors

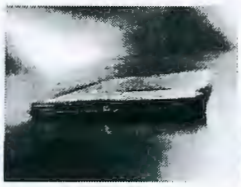


RQS nº 03/2005 - CN
CPMI - CORREIOS
1074
Fls. Nº
3690
Doc

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Product Specifications

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
				
Performance	80 Mbps	250 Mbps	500 Mbps	1000 Mbps
Standard monitoring interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	Dual 1000BASE-SX interface with MTRJ
Standard command and control interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional interface	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	-1000BASE-SX (fiber) -Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	1000BASE-SX (fiber)
Performance upgradable	No	No	Yes	No
Form factor	One rack unit	One rack unit	One rack unit	One rack unit
Advanced protection algorithms				
Stateful pattern recognition	Yes	Yes	Yes	Yes
Protocol parsing	Yes	Yes	Yes	Yes
Heuristic detection	Yes	Yes	Yes	Yes
Anomaly detection	Yes	Yes	Yes	Yes
Attack protection				
Sweeps or floods	Yes	Yes	Yes	Yes
Denial-of-service (DoS) mitigation	Yes	Yes	Yes	Yes
Worms or viruses	Yes	Yes	Yes	Yes
Common gateway interface (CGI) or WWW attacks	Yes	Yes	Yes	Yes
Buffer overflow protection	Yes	Yes	Yes	Yes

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1075
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Remote-procedure call (RPC) attack detection	Yes	Yes	Yes	Yes
IP fragmentation attacks	Yes	Yes	Yes	Yes
Internet Control Message Protocol (ICMP) attacks	Yes	Yes	Yes	Yes
Simple Message Transfer Protocol (SMTP), Sendmail, Internet Message Access Protocol (IMAP), or Post Office Protocol (POP) attacks	Yes	Yes	Yes	Yes
File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Telnet, and rlogin attacks	Yes	Yes	Yes	Yes
Domain Name System (DNS) attacks	Yes	Yes	Yes	Yes
TCP hijacks	Yes	Yes	Yes	Yes
Windows or NetBios attacks	Yes	Yes	Yes	Yes
TCP application protection	Yes	Yes	Yes	Yes
BackOrifice attacks	Yes	Yes	Yes	Yes
Network Timing Protocol (NTP) attacks	Yes	Yes	Yes	Yes
Customizable signatures using Signature Micro-Engine technology	Yes	Yes	Yes	Yes
Automated signature updates	Yes	Yes	Yes	Yes

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1076
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Alarm summarization	Yes	Yes	Yes	Yes
Support for 802.1q traffic	Yes	Yes	Yes	Yes
P2P / file sharing detection techniques	Yes	Yes	Yes	Yes
Secure communication				
IP Security (IPSec) or Secure Sockets Layer (SSL) between sensor and management console	Yes	Yes	Yes	Yes
Encrypted signature packages	Yes	Yes	Yes	Yes
SSH for remote administration	Yes	Yes	Yes	Yes
Serial Control Protocol (SCP) support for secure file transfer	Yes	Yes	Yes	Yes
IDS evasion protection				
IP fragmentation re-assembly	Yes	Yes	Yes	Yes
TCP stream re-assembly	Yes	Yes	Yes	Yes
Unicode deobfuscation	Yes	Yes	Yes	Yes
Active response actions				
Router access-control-list (ACL) modifications	Yes	Yes	Yes	Yes
Firewall policy modifications	Yes	Yes	Yes	Yes
Switch ACL modifications	Yes	Yes	Yes	Yes
Session termination via TCP resets	Yes	Yes	Yes	Yes
IP session logging or session replay	Yes	Yes	Yes	Yes

ECT 1627 CPL - AC

RQS nº 03/2005 - CN CEMI - CORREIOS
Fls. Nº 1077
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Active notification actions				
Alarm display	Yes	Yes	Yes	Yes
E-mail alerts	Yes	Yes	Yes	Yes
E-page alerts	Yes	Yes	Yes	Yes
Customizable script execution	Yes	Yes	Yes	Yes
Multiple alarm destinations	Yes	Yes	Yes	Yes
Third-party tool integration	Yes	Yes	Yes	Yes
IDS active update bulletins	Yes	Yes	Yes	Yes
Administration				
Web user interface (Secure Hypertext Transfer Protocol [HTTPS])	Yes	Yes	Yes	Yes
Command-line interface (CLI) (console)	Yes	Yes	Yes	Yes
CLI (Telnet or SSH)	Yes	Yes	Yes	Yes
CiscoWorks VPN Security Management Solution (VMS) support	Yes	Yes	Yes	Yes
High availability				
Redundant power supply	No	Yes	Yes	Yes
Failure detection				
Monitoring link failure detection	Yes	Yes	Yes	Yes
Communications failure detection	Yes	Yes	Yes	Yes
Services failure detection	Yes	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes	Yes
Dimensions				

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1078
Doc. 3690

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Height	1.7 in. (4.37 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)
Width	16.8 in. (42.72 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)
Depth	11.8 in. (29.97 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)
Weight	11.5 lb (4.11 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)
Rack-mountable	Yes	Yes	Yes	Yes
Power				
Autoswitching	100V to 240V AC	110–220 VAC	110–220 VAC	110–220 VAC
Frequency	50 to 60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Operating current	1.5A	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V
Operating environment				
Operating temperature	+5°C to +40°C (+41°F to +104°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)
Nonoperating temperature	-25°C to +701/4°C (–13F to +1581/4°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)
Operating relative humidity	5 to 95% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation (most severe case with full power usage)	410 Btu/hr (full power usage (65W))	983 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)

Note:

- This 80-Mbps performance for the Cisco IDS 4215 is based on the following conditions:
  - 800 new TCP connections per second
  - 800 HTTP transactions per second
  - Average packet size of 445 bytes,
  - Running Cisco IDS 4.0 Sensor Software
- This 250-Mbps performance for the Cisco IDS 4235 is based on the following conditions:
  - 3000 new TCP connections per second
  - 3000 HTTP transactions per second
  - Average packet size of 445 bytes

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1079
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Running Cisco IDS 4.0 Sensor Software
- This 500-Mbps performance for the Cisco IDS 4250 is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 445 bytes
  - Running Cisco IDS 4.1 Sensor Software
- This 1000-Mbps performance for the Cisco IDS 4250-XL is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 595 bytes
  - Running Cisco IDS 4.0 Sensor Software

Regulatory Compliance

- EMC—FCC (CFR 47 Part 15) Class A, CISPR 22 Class A, EN 55022 Class A, EN 55024, EN61000-3-2, EN61000-3-3, VCCI Class A, AS/NZS 3548 Class A, CE marking
- Safety UL 60950, CSA 22.2 No.60950, IEC 60950, EN 60950, AS/NZS 3260, CE marking.

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
IDS-4215-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector), 80-Mbps
IDS-4215-4FE-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector plus 4FE interface card), 80-Mbps
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-TX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-SX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 1000BASE-SX with SC connector)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator, with dual 1000BASE-SX and MTRJ connectors)
IDS-XL-INT=	Cisco IDS Accelerator Card with dual 1000BASE-SX interfaces and MTRJ connectors
IDS-4250-SX-INT=	1000BASE-SX monitoring interface with SC connector
IDS-4FE-INT=	Spare 4FE (10/100 BaseTx) sniffing interfaces for 4215, 4235, & 4250
IDS-PWR=	Spare power supply for the Cisco IDS 4235 and 4250 sensors
IDS-SCSI=	Spare Small Computer Systems Interface (SCSI) hard disk drive for Cisco IDS 4250 Sensor
IDS-RAIL-2=	Two post rail kits for the Cisco IDS 4235 and 4250 sensor platforms
IDS-RAIL-4=	Four post rail kits for the Cisco IDS 4235 and 4250 sensor platforms

ECT 1012 A

ECT nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1080
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4215XK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-SNTE-IDS4215XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-SNTP-IDS4215XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-OS-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-OSE-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-OSP-IDS4215XK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-SNT-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-SNTE-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNTP-IDS4215-4FEXK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-OS-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-OSE-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-OSP-IDS4215-4FEXK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNT-IDS4235K9	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4235)
CON-SNTE-IDS4235K9	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4235)
CON-SNTP-IDS4235K9	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4235)
CON-OS-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4235)
CON-OSE-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4235)
CON-OSP-IDS4235K9	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4235)
CON-SNT-IDS4250TK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-SNTE-IDS4250TK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-TX)
CON-SNTP-IDS4250T	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-OS-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-OSE-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x 4 Cisco (IDS 4250-TX)
CON-OSP-IDS4250TK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-SNT-IDS4250SK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-SX)
CON-SNTE-IDS4250SK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-SNTP-IDS4250SK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-OS-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-SX)
CON-OSE-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-OSP-IDS4250SK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-SNT-IDS4250XK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-XL)
CON-SNTE-IDS4250XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-SNTP-IDS4250XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-XL)
CON-OS-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-XL)
CON-OSE-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-OSP-IDS4250XK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-XL)

RQS nº 03/2005 - CN
CPMI - CORREIOS
1001
Fls. Nº
Doc: 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4FE	Cisco SMARTnet support 8 x 5 x NBD (IDS-4FE-INT=)
CON-SNTE-IDS4FE	Cisco SMARTnet support 8 x 5 x 4 (IDS-4FE-INT=)
CON-SNTP-IDS4FE	Cisco SMARTnet support 24 x 7 x 4 (IDS-4FE-INT=)
CON-OS-IDS4FE	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-4FE-INT=)
CON-OSE-IDS4FE	SMARTnet onsite support 8 x 5 x 4 (IDS-4FE-INT=)
CON-OSP-IDS4FE	SMARTnet onsite support 24 x 7 x 4 (IDS-4FE-INT=)
CON-SNT-IDSXL	Cisco SMARTnet support 8 x 5 x NBD (IDS-XL-INT=)
CON-SNTE-IDSXL	Cisco SMARTnet support 8 x 5 x 4 (IDS-XL-INT=)
CON-SNTP-IDSXL	Cisco SMARTnet support 24 x 7 x 4 (IDS-XL-INT=)
CON-OS-IDSXL	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-XL-INT=)
CON-OSE-IDSXL	SMARTnet onsite support 8 x 5 x 4 (IDS-XL-INT=)
CON-OSP-IDSXL	SMARTnet onsite support 24 x 7 x 4 (IDS-XL-INT=)

Export Considerations

The Cisco IDS 4200 Series sensors are subject to export controls. Refer to the export compliance Web site for guidance at: http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco Intrusion Protection System, go to: http://www.cisco.com/go/ids

For more information about the CiscoWorks VMS Solutions (IDS management), go to: http://www.cisco.com/go/vms

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1082
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

E C T
CPL - AC

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
0189
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW4599 0503

E C T
1619
SEL - AC

Intrusão doc 2

RQS nº 03/2005 - CN
CPMI - CORREIOS
1084
Fls. Nº
3690
Doc:

Cisco Secure Intrusion Detection System

General Concepts

Q. What is the Cisco Secure Intrusion Detection System, formerly known as NetRanger™ ?

A. Network intrusion detection is a process that identifies and responds to misuse or policy violations on a network. By placing Sensor devices at determined points on the network, network traffic is monitored and compared against patterns or "signatures" that represent suspicious activity, misuse, or actual attacks. The Sensor can send alerts to the Director, a security management system, and, under appropriate circumstances, send commands directly to network equipment such as routers and firewalls, reconfiguring them to deny access to the attacker. The system automatically and quickly responds in a user-defined manner to send an alert or take immediate action.

Q. What is the difference between network-based and host-based intrusion detection?

A. Host-based intrusion detection monitors activity on a single system while network-based intrusion detection monitors all activity over a given network connection or segment. Host-based intrusion detection systems are used to protect critical network servers or other individual systems containing sensitive information. The implementation of these systems is in the form of small clients or applications. Host-based systems require the use of a host server's system resources—disk space, RAM, and CPU time, and it impacts system performance. Intrusions are detected by analyzing operating system audit trails, application audit trails, and other system activity. Host-based intrusion detection systems are ideal if a limited number of critical servers must be protected, but they do not scale well if enterprise-wide solutions are needed.

Network-based intrusion detection systems are used to monitor activity on a specific network segment. Whereas a host-based intrusion detection system resides on a workstation and shares CPU with other user applications, a network-based solution is a dedicated platform. Network-based intrusion detection systems perform a rule-based or expert system analysis of traffic using parameters set up by the security manager, and the signatures, which flag suspicious or attack activity. The systems analyze network packet headers to make security decisions based on source, destination, and packet type. They also analyze packet data to make decisions based on the actual data being transmitted. These systems scale well for network protection because the number of actual workstations, servers or user systems on the network is not critical—the amount of traffic is what matters. In addition, sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise. The Cisco Secure Intrusion Detection System, a network-based intrusion detection system provides network administrators with enhanced security technology and capabilities to secure their networks.

Q. How does the Cisco Secure Intrusion Detection System (IDS) fit into the Cisco end-to-end security strategy?

Public
Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1085
3690
Doc.

A. As the dynamic security component of the Cisco end-to-end security product line—which includes firewalls, encryption, authentication, and active audit—intrusion detection enables customers to monitor users in nearly all network traffic or activity. At the sign of suspicious activity, the Cisco Secure IDS responds in real time according to the designated security policy. When used in conjunction with firewalls, encryption, authentication, and active audit, the system allows customers to build and operate secure electronic business environments.

Q. How does the Cisco Secure IDS differ from firewalls?

A. The Cisco Secure IDS complements firewalls and other security devices. The firewall's function is access control, integrity, and enforcing security policy. If someone attempts a violation, the Cisco Secure IDS dynamically responds to the security policy violations and eliminates unauthorized activity in real time. The active audit capabilities of the Cisco Secure IDS provide an excellent complement to firewalls, much like burglar alarms and motion detectors complement physical access controls such as door locks and window bars.

Misuse is often perpetuated by a company's own employees or hackers masquerading as trusted users. The Cisco Secure IDS provides the ability to monitor network-related traffic from these trusted users to prevent network breaches from inside as well as outside the company.

Q. How does the Cisco Secure IDS work with firewalls, and where are Sensors typically located relative to a firewall?

A. The Cisco Secure IDS works with firewalls, but currently does not directly communicate with them. Sensors can be placed "behind" a firewall (such as between the protected network and the firewall), or "in front" of a firewall (such as between the firewall and the perimeter router). In all implementations, the Sensor is monitoring via a promiscuous tap on the line and DOES NOT constitute a point of failure if the device stops operating.

The most common location for the Sensor is in front of the firewall. In this position the Sensor can monitor not only outbound traffic, but activity that would be blocked by the firewall. Seeing all the activity targeting the protected network provides information for security operators to adjust policies and security products to best protect the network.

Sensors are usually only placed behind a firewall to ensure trusted user traffic coming through the firewall complies with security policy and to verify the firewall is properly blocking inbound traffic. While the Sensor can see all packets flowing out of the local network, it can only see inbound packets allowed by the firewall policy.

Q. Where, besides locations that already contain firewalls, would I place a Sensor?

A. There are two generally accepted locations for an intrusion detection sensor—the network perimeter and the internal network. The perimeter includes all Internet access points, where a firewall is traditionally situated. However, intrusion detection may be just as important to your security policy in other access points, such as the network side of a modem pool or at business- partner network connections, where firewall implementations are less common. Sensors may be installed on any network segment that is critical to your enterprise operation. For example, a link between engineering and finance departments can be monitored to ensure that your corporate security policy is enforced and that critical resources, such as sensitive data storage or Web service are protected. The Cisco Secure IDS can scale to meet your needs so that as the network grows, additional sensors can be installed to provide a secure solution.

Q. How does the Cisco Secure IDS operate in a switched environment?

A. In its current appliance form, the Cisco Secure IDS Sensor can be placed on the switch SPAN port to monitor network traffic. Implemented in this way, the Sensor can monitor any virtual LAN segment that has been configured in the switch to be copied to the SPAN port.

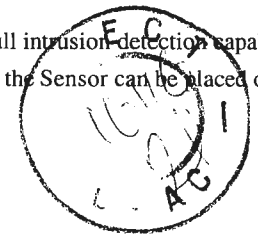
Q. Does the Cisco Secure IDS still work if the network traffic is encrypted (for example, IPSec, and SSL)?

A. The Cisco Secure IDS Sensor analyzes both packet header information and packet data information to determine if suspicious activity is occurring. Encryption algorithms encrypt the data portion of the packet for confidentiality. Since it can only process what it can "see," the Sensor can not detect attacks that require inspection of the payload or data fields within a packet. It will, however, still alarm and respond to attacks, which are detected from the unencrypted packet header information. All network-based intrusion detection systems suffer this

RQS nº 03/2005 - CN
CPMI -- CORREIOS
Fls. Nº 1086
3690
Doc.

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

problem. Therefore, in networks carrying encrypted traffic, Sensor placement is critical. To use their full intrusion-detection capability, the Cisco Secure IDS Sensors should be installed where the traffic has already been decrypted. Otherwise, the Sensor can be placed on an encrypted segment and will detect all but the packet data or payload-based attacks.



Architecture

Q. What is the Cisco Secure IDS architecture?

A. The Cisco Secure IDS comprises of at least one Director and one or more Sensors. Cisco Secure IDS Sensors in distinct network locations protect enterprise-wide TCP/IP networks by detecting, responding to, and reporting unauthorized activity. Directors collect incoming Sensor data, translate it, and present it to security personnel in an intuitive, map-oriented graphical user interface. Directors also allow security personnel to manage configurations of remote Sensors. Directors can also manage Sensor data by exporting it to third-party relational databases. The Sensors in the base package can perform TCP resets on sessions exhibiting suspicious activity. Cisco offers an optional software package for each Sensor, called device management, which can dynamically change access control lists (ACLs) on Cisco routers to block suspicious activity.

Q. What is the rationale behind this architecture?

A. The response times of an intrusion detection system can vary considerably depending on many factors. Since the Cisco Secure IDS uses inband communications to the Director, it is subject to normal network lag. Therefore, Cisco's philosophy has been to place the "intelligence" esponse (the Cisco Secure IDS Sensors) in locations where it can respond most effectively. By placing a Sensor physically close to the routers it is communicating with, and in front of the network it is protecting, the Sensor can quickly perform resets and shuns to protect its network. Alarm transmissions to the Director and operator, while still important, are a secondary consideration. The Sensor typically responds in fractions of a second, while an operator can take minutes leaving a window for the attacker to cause problems.

Q. What types of suspicious activities does the Cisco Secure IDS detect?

A. The Cisco Secure Intrusion Detection System engine uses a signature recognition methodology, which can be context and content oriented. Context-oriented attack signatures consist of known network service vulnerabilities that can be detected by inspecting packet headers. These include SATAN, TCP Hijacking, and IP spoofing attack profiles. Content-oriented signatures require the inspection of the payload or data fields within a packet to determine if an attack or policy violation has occurred at the application level.

These include e-mail and Web attack profiles for example.

Cisco Secure IDS signatures can be grouped into three categories:

- *Name Attacks*—those with specific names such as Smurf and PHF.
- *General Category Attacks*—attacks with many variations, but based on the same basic exploit, such as out-of-band data (Teardrop) or IP fragmented packets. This simplifies signature management and provides perpetual protection against new attack variations, which would otherwise go undetected.
- *traordinary Attacks*—extremely complex signatures such as Simplex-Mode TCP hijacking, Loki, or e-mail Spam.

The Cisco Secure IDS also enables customers to create customized character string matching signatures to meet specific operational or business requirements. For example, XYZ Corporation could easily configure the Cisco Secure IDS to send an alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or FTP.

Q. Will the Cisco Secure IDS detect attacks if the hacker uses signatures not in the signature database?

A. It depends upon the type of attack, but in most cases they will be detected. Hackers can rarely, if ever, break into systems and use signatures that will not be recognized by the Cisco Secure IDS. The Cisco Secure IDS is optimized to detect the reconnaissance and probing efforts of hackers, typically precursors to an actual attack. Most of the General Category signatures are developed for just this purpose—to detect common variations on a system exploit.

Q. Can't the user customize the product and add their own signatures as well?

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

A. Customers can define custom string-match signatures. Cisco Secure IDS users can easily develop custom string-based signatures for immediate defense from certain attacks. This same capability can be used to search for data unique to the customer environment. For example, XYZ Corporation could easily configure the Cisco Secure IDS to alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or FTP.

Q. How secure is the system itself from attack?

A. The Cisco Secure IDS Sensor is built to protect it itself from attack. To start, only services required by the Sensor are enabled. Second, TCP wrappers ensure that communication is allowed only with the Director. Third, the Sensor detects attacks across the monitored segment including any that may be directed at it. And, finally, the Sensor can be "invisible" to the network when its monitoring interface is in promiscuous mode, and its command and control interface is assigned to a dedicated router interface or connected into the protected network behind a firewall. The Director was designed to be placed on a trusted network and therefore only uses standard operating system and application-level security. The Director could be configured with third party products to use certificates for authentication during console log on. It should be placed on a network segment that is either directly or indirectly monitored by a Sensor for optimum protection.

Q. Is the information passed between the Sensor and Director encrypted and authenticated?

A. The Cisco Secure IDS does not currently support Sensor to Director encryption, but relies on router-to-router IPSec encryption to protect security information as it crosses the WAN. All communication between the Sensor and Director is natively authenticated to ensure communications have not been spoofed or hijacked.

Q. What types of networks can be connected to the monitoring and control interfaces on the Sensor?

A. Each Sensor comes with two interfaces—one used for monitoring the desired network segment for suspicious activity and one used for control from the Director. The control interface is 10/100base T Ethernet. The monitoring interface options include Ethernet, Token Ring, Fast Ethernet, Single Attached FDDI, and Dual Attached FDDI, and are used to determine the appropriate model when ordering.

Operations

Q. Where within the system are the various operational functions performed?

A. The Sensor is a rules-based system, it monitors network activity and takes action in real time depending on its configuration parameters. It is a dedicated "black box" appliance on the network and monitors and analyzes the raw network data. It can send an alarm, log an event to disk, issue a TCP reset command to reset a session, and issue a command to change an ACL on a Cisco router—blocking or shunning the suspicious activity. All these options are configurable to meet the operations staff needs. All Sensor management is conducted from a Director workstation. These workstations can be set up in a redundant or hierarchical fashion to ensure they meet operational needs. Generally, a second workstation is set up with the Director to provide database storage of alarm information and to be used as an analysis workstation for trend and historical information that requires database-intensive queries.

Q. How will a network operator know when an attack occurs?

A. The Cisco Secure IDS Director console displays color-coded icons for each Cisco Secure IDS Sensor that it manages. The Sensor immediately transmits alarm information over a reliable, communications protocol when it detects an attack. In turn, the color of the Sensor representative icon on the Director console changes (typically from green to yellow to red) depending on the severity of the attack. Users can specify the levels of alarms based on their business operations. By drilling down on the respective icon, users can investigate details of the attack, including the attack type, its electronic point of origin, the attack's destination address and port, and, in many cases, the 256 keystroke characters that preceded the attack.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1088
Doc 3690

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

In addition to the Sensor sending alarms sent from the intrusion detection algorithms of the Sensor, the Sensor can send alarms based on ACL violations on Cisco routers. The Sensor and the router can be configured such that when an ACL on a router generates a syslog entry, the information is also forwarded to a Sensor—which in turn passes it as an alarm to the Director. This provides the network operator additional visibility into activity that is occurring on the network.

Q. Besides the Cisco Secure IDS Director interface, how can an operator be notified of security events?

A. The Cisco Secure IDS supports paging and e-mail notification in addition to the visual icon changes. Because the Director is closely integrated into Hewlett Packard OpenView, it can be used to generate Simple Network Management Protocol (SNMP) traps for any event sent in from a Sensor. These SNMP traps, in turn, can be used to start custom applications or activate scripts, generate an entry in a trouble ticket system, or activate any number of user defined activities.

Q. What are the default values assigned to signatures in the system and what is the process used to research an event?

A. The Cisco Secure IDS assigns default values of 1 to 5 on all signatures/event information that it detects and logs. Users can define up to 255 different alarm levels. Typically, Level 1 events are logged at the Sensor only. Level 2 events and above are more likely to have security relevance and are transferred to the Director for operator consideration. Level 2 or 3 alarms are displayed with a yellow icon on the Director while more severe Level 4 or 5 alarms are red. If the operator determines an event is suspicious, he can pull the Level 1 log from the Sensor for additional detail. At this point, the operator may access all available system data and can query the database for specific information. The Cisco Secure IDS includes Oracle database templates and several SQL-based queries to provide a user a "quick start" with the analysis. Most customers have other tools that work with Oracle, which they have tailored for the research and reporting they desire. The operator may also consult with the HTML-based Network Security Database (NSDB) which gives additional information on security events and their ramifications.

Q. How are the signatures maintained and updated?

A. Cisco will place signature updates on Cisco Connection Online (CCO) every other month (additional releases may be required in extraordinary situations). Customers with maintenance agreements can access to these signatures and download them to the Director. From the Director, the operator can "push" the new signatures out to the Sensors. This push will only update the Sensor with the new signatures and will not overwrite any changes the operator may have made in customizing the configuration.

Q. How does the system respond in the event of a power outage or network connectivity problem?

A. Cisco Secure IDS Sensors automatically reboot and attempt to establish communications with the Director after a power outage. The Director will display an alarm when Sensor connectivity is lost. The Sensors can be configured to switch to secondary and tertiary network paths back to their Directors, or a Sensor can be configured to establish connectivity with an alternate Director. If this is still not possible, a Sensor will queue and store the event information until the link is reestablished. The Sensor will continue to operate effectively even if the Director link is lost; for example it will perform TCP resets, ACL changes, paging, and so forth. Once connectivity is reestablished, the queued information will be forwarded and displayed on the Director.

What happens if a Sensor fails?

A. The Director monitors the health of a Sensor via a continuous heartbeat. If the Sensor can not communicate for more than one minute, an alarm is created by the Director indicating a communications problem with the Sensor. If it is determined that a Sensor has failed, it can be replaced by another Sensor appliance and the configuration, stored in the Director's Configuration Library, can be quickly downloaded.

Q. How is the system fine-tuned to reduce false positive signatures?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1089
Doc 3690

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

A. Each Sensor database signature is tested extensively to ensure that when network activity of a given type occurs, the signature will "fire" and send an alarm. False positives occur when a legitimate system activity sets off an alarm; for example a network management system may send out a series of pings to determine if other systems are active on the network. The Cisco Secure IDS can reduce false positives by deselecting specific signatures from specific addresses. For the network management system in the example using a discovery feature that includes regular ping sweeps, the user can deselect ping sweeps from that address in the Cisco Secure IDS configuration. However, any other attacks that originate from that device will be discovered. This provides a fine level of granularity in fine-tuning the system for optimum security operations.

Service and Support

Q. How is the Cisco Secure IDS intrusion detection system packaged?

A. The Sensors are packaged as network "appliances," which come with all necessary software preloaded. Installation is accomplished at the technician level, provided network information for the device is available on site or in advance, such as IP address, network mask, host name, and so forth. The Director is packaged as a software module and requires HP OpenView Network Node Manager. The Director software also provides the tools to load the Cisco Secure IDS information into an Oracle relational database, where it can be retrieved for reporting or analyzed for historical and trend activity. The database should be installed on a separate machine for performance and operational reasons.

Q. What type of Cisco service and support is provided for the Cisco Secure IDS?

A. The Cisco Secure IDS Sensor is covered by all six levels of SMARTnet™ maintenance. This includes hardware support as well as Sensor software upgrades and access to the latest signatures posted on CCO. The Director software is covered by Software Application Support (SAS) and Software Application Support Plus Upgrades (SAU).

Q. How are the Sensors and Director software installed?

A. The Sensors were designed for technician-level installation, requiring the appliance to be simply plugged into the network, turned on, and configured with several simple parameters. These parameters include standard network items such as IP address, host name, network masks, Director IP address, and so forth. Once completed, the Sensor begins protecting the network with a default intrusion detection policy. The Director software is loaded on the workstation with the help of an installation wizard. Once operational, the Director will prompt the operator to begin establishing communications with the Sensors. As each Sensor is contacted, the default configuration parameters are pulled back to the Director and the operator will be prompted to customize the security policy for that Sensor. Once the operator is finished setting up the new policy parameters, they are stored on the Director and pushed back out to the Sensor, where they are immediately enforced.

Q. How is field support provided for the Sensors?

A. Replacement of the Sensors is performed via complete unit replacement. The technician will install a new Sensor and the current policy from the Director will be pushed out to the new Sensor. Software upgrades and signature updates will be pushed out to the Sensors in the same way. Software upgrades will be available on CCO for all customers who purchase system maintenance.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1090
Fls. Nº
Doc.

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

ECT
CPL - AC

Cisco Systems

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

RQS nº 03/2005 - CN
CPMI - CORREIOS
1091
Fls. Nº
Doc. 3690

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the
Cisco Connection Online Web site at http://www.cisco.com/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia México • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 1998 Cisco Systems, Inc. All rights reserved. Printed in USA. NetRanger and SMARTnet are trademarks, Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9810R)
12/98 B&W

E C T I

Intrusão doc 3

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1092
3690
Doc.

Cisco Systems

DATA SHEET

Cisco **IDS 3.0** Sensor Software for Cisco 4200 Series Appliances

The industry-leading Cisco IDS Intrusion Detection System solution provides customers with unmatched intrusion protection technology through the Cisco Active Defense System. The integrated hardware and software solution delivers best-of-breed protection for both perimeter and internal resources.

Version 3.0 is the latest release of the Cisco IDS application software for the Cisco 4200 Series appliances. It delivers the latest in innovative IDS features, including Active Update signature distribution mechanisms, customizable signature language, extensions to the Active Response capabilities, and secure administration.

Key Features and Benefits

Signature Definition and Distribution Enhancements

Active Update Mechanism

Cisco IDS now 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.

Signature Instruction Language for Verifying Exploits and Reconnaissance (SILVER)

Cisco IDS continues to innovate with the release of the Cisco SILVER signature language. Users can now develop custom signatures spanning Layer 2 through Layer 7 attributes. Developed by the Cisco Countermeasures Research Team, SILVER is the mechanism that this team uses to develop all new signatures for the IDS product. Now Cisco is exposing this capability to its customers, providing them unparalleled flexibility to develop new signatures.

This new language also decreases the time between signature releases because the signatures can be released as update files rather than compiled in the core sensor binary. Similar to antivirus products, the signature engines and the data files can be released separately.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1093
Fls. Nº
3690
Doc.

Cisco Systems, Inc.
All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Tunable Signatures

One of the challenges of event monitoring for IDS is to reduce the occurrence of false positives, thereby allowing the user to focus only on alarms that are deemed security relevant. However, because the security objectives for each IDS deployment are unique, Cisco IDS 3.0 adds granularity to the way in which sensors may be tuned to specifically suit the environment in which they are deployed. Users may now tune signature threshold parameters to meet their unique security objectives. For example, for the ping sweep signature, the user can now define the number of hosts pinged before the signature fires.

Alarm Summarization

Attackers may use tools such as Stick to cause sensors to send numerous alarms to management consoles as a way of flooding the management console. The Alarm Throttle feature in Cisco IDS 3.0 allows users to consolidate alarms to a single event, thereby preventing the management console from being overwhelmed with numerous events. For example, if the rate of alarms being sent by the sensor exceeds a certain threshold value, the signature may be set to automatically throttle to a summarization mode to produce a single alarm that comprises numerous alarm firings. A time interval may also be specified that determines the rate at which subsequent consolidated alarms are sent to the management console.

Detection of Network DoS Attacks

Cisco IDS 3.0 adds functionality to detect network denial-of-service (DoS) attacks that are targeted at consuming network resources. An inspector monitors the data capture by maintaining a counter that tracks the number of packets being captured per second. If the rate of packets being captured exceeds a specified rate and such peaks occur at a certain frequency, an alarm is generated to alert the user of a possible DoS attempt.

Active Response Extensions

Shunning with the Cisco PIX Firewall and Cisco Catalyst Switches

Cisco IDS incorporates proactive response functionality into the sensor appliances by allowing users to configure the IDS to dynamically respond to an attacking host by preventing new connections and disallowing packets from any existing connection. Cisco IDS 3.0 extends this Active Response capability beyond Cisco routers into a wide range of Cisco's high-performance networking devices, including the Cisco PIX® Firewall (running PIX 6.0+), Cisco Catalyst® 6000 Switch, and Cisco Catalyst 5000 Switch. This shunning gives security operators unparalleled control to reach across the network to quickly stop misuse and end intruders' access to the network.

Interoperability with Existing ACLs

Shunning is accomplished by the dynamic modification of access control lists (ACLs) on managed devices. Cisco IDS 3.0 allows the user to configure the sensor to shun while maintaining any user-defined access control entries on the specified interface and direction.

Secure Administration

In addition to existing functionality that provides secure communications between the sensor and the management console using IP Security (IPSec), Cisco IDS 3.0 also supports the Secure Shell Protocol (SSH) to allow users to remotely access sensors over a secure connection.

IP Session Replay

IP session logging provides extensive logging that is important for system troubleshooting as well as for reconstructing system events before and after attacks. Cisco IDS 3.0 augments this existing capability by converting these logs to a standard TCP dump format that allows them to be viewed and replayed using public domain utilities, such as Ethereal and TCPReplay.

Enhanced Filtering

Users have the ability to specify which source or destination IP addresses that specified signatures must alarm on. Because certain signatures may be classified as security relevant for certain source or destination IP addresses and yet do not need to be analyzed for other IP addresses, this level of enhanced filtering minimizes the occurrence of false positives.

Alarm Generation When Sniffing Interface is Disconnected

Sensors are equipped with a monitoring interface for data packet capture and a command and control interface for transmitting alarms to the management console and receiving configuration information from the

ECT ... AC
Fls. Nº 1094
CORREIOS

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

management console. With Cisco IDS 3.0, when the sniffing interface is disconnected, an alarm is triggered. This setup provides the user with an alert mechanism when the interface is tampered with and hence assures persistent operation.

Technical Specifications

Ordering Information

SMARTnet™ customers may download Cisco IDS 3.0 from Software Center on CCO at http://www.cisco.com

Part number for IDS Software Upgrade for Non-Support Customers: IDS-SW-U

Export Considerations

IDS sensors are subject to export controls. Please refer to the export compliance Web site at

http://www.cisco.com/wwl/export/crypto/ for guidance.

For specific export questions, please contact export@cisco.com.

Additional Information

Cisco Secure Intrusion Detection System:

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

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

European Headquarters
Cisco Systems 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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. SMARTnet is a trademark of Cisco Systems, Inc.; and Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

LW2654 09/01

Printed in the USA

ECT
CPL - AC

ROS n° 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1090
3690
Doc.

Intrusão doc 4

RQS nº 03/2005 - CN
CPMI - CORREIOS
1096
Fls. Nº
Doc. 3690

Cisco Intrusion **Detection** System

Q. What is a "network-based" IDS?

A. Two basic types of IDSs are on the market today: host-based and network-based systems. The fundamental difference between them is the source of the activity that they monitor and analyze to detect intrusions. Host-based IDSs monitor activity on a host or end system, while network-based IDSs monitor network traffic. Host-based IDSs are used to protect critical network servers or other individual systems containing sensitive information.

Network-based IDSs are used to monitor activity on a specific network segment. Whereas a host-based IDS resides on a workstation and shares CPU with other user applications, a network-based solution is a dedicated platform. Network-based IDSs perform a rule-based or expert system analysis of traffic using parameters set up by the security manager, and the signatures, which flag suspicious or attack activity. The systems analyze network packet headers to make security decisions based on source, destination, and packet type. They also analyze packet data to make decisions based on the actual data being transmitted. These systems scale well for network protection because the number of actual workstations, servers, or user systems on the network is not critical, the amount of traffic is what matters. In addition, sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise. The Cisco® network-based Intrusion Detection System provides network administrators with enhanced security technology and capabilities to secure their networks.

Q. If I already have a firewall, do I really need an IDS?

A. Absolutely. Although an IDS will not replace your firewalls or other security devices for that matter, it serves a very complementary role and addresses certain risks that firewalls cannot. The primary function of the firewall is to control access to services and hosts based on your site security policy. If a service or connection to a specific host is permitted, firewalls typically permit all such traffic, and they do not inspect the content of the permitted traffic. An example is permitting public access to a Web server on a DMZ. All connection requests to the Hypertext Transfer Protocol (HTTP) port on that Web server will be permitted by the firewall, including malicious traffic directed at the HTTP server to exploit a buffer overflow vulnerability. Although most firewalls will not protect against data/content-driven attacks (for example, buffer overflow), IDSs will. Furthermore, firewalls typically will not protect you against attacks originating from inside your network or entering your environment from other ingress points not protected by firewalls (for example, remote access servers). IDSs can be strategically deployed to monitor activity from internal sources and other network ingress points without impacting your network. Deploying an IDS to complement your firewall(s) will significantly enhance your security posture.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1097
Fls. Nº
Doc. 6090

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. Is there a mechanism by which users may contact the IDS Product Team at Cisco?

A. Yes. Users may pose questions, requests, and comments to the following e-mail address:

ids-news@cisco.com

In addition, users have the ability to share experiences with other users and also pose questions to the Cisco IDS Engineering & Product Marketing teams at the IDS Networking Professionals Forum at:

http://forums.cisco.com/eforum/servlet/
NetProf?page=netprof&CommCmd=MB%3FcmdDdisplay_messages26mode3Dnew26location%3D.ee6e1fc

Q. Does anyone offer a managed IDS service using the Cisco IDS?

A. Yes, numerous managed service providers offer a managed IDS service using the Cisco IDS. These managed service providers include AT&T, Counterpane, IBM Emergency Response Services, NetSolve, Riptech, RedSiren, and Ubizen.

Sensors

Q. What are the new features of the Cisco IDS 4.0 Sensor software?

A. The Cisco IDS 4.0 Sensor software delivers a number of new features and enhancements to the network-based IDS portfolio. These features include:

- Re-architecture of communications protocol to enhance the efficiency of message transactions
- Common code base to allow feature parity between the appliance sensor and the switch sensor
- Delivery of a Layer 2 signature engine to mitigate issues such as man in the middle attacks and ARP spoofing in switched environments
- Introduction of an SMB engine to efficiently address attacks related to SMB
- Ability to capture the trigger packet that caused an alarm
- Enhanced shunning capabilities to allow shunning by port address
- Major enhancements to our existing protocol anomaly techniques
- Provision of Analysis Statistics Engine to deliver information of metrics such as bad checksums, bytes processed, data rates Mbps, TCP nodes per sec, and other analysis metrics
- Introduction of a full featured Cisco IOS-like CLI (command-line interface) for unprecedented sensor management over a secure SSH connection
- Capability of capture and display of the VLAN ID of the malicious traffic that was detected
- Enhancements to IP Fragmentation Reassembly
- Higher levels of granularity for the alarm information that is transmitted to the management console
- Support for ntp
- NAT support
- Logical signature groupings to allow global changes across the groupings
- Ability to implement exceptions to filter events to be displayed
- Tunability of IP session logging parameters

RQS nº 03/2005 - CN
CPMI - CORREIOS
1098
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. What performance numbers (Mbps) are supported by the Cisco IDS Sensors?

A. The Cisco IDS 4215 supports 80 Mbps of performance and can be used to protect T1/E1/T3 environments.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces, it can also be deployed on partially utilized gigabit links.

The Cisco IDS 4250 supports superior performance at 500 Mbps and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets.

Intrusion protection for fully saturated gigabit links is delivered by the Cisco IDS 4250-XL. Using customized hardware acceleration, the IDS-4250-XL can be used to protect gigabit subnets and multiple partially utilized gigabit links.

The Cisco Catalyst® 6500 Series Intrusion Detection System (IDSM-2) Services Module supports 600 Mbps. This module operates within the Catalyst 6500 Series and provides protection for traffic traversing the switch, which could be traffic from a single subnet or from numerous subnets that are being aggregated through the switch.

The Cisco IDS Network Module provides full-featured Intrusion Protection that is integrated into the Cisco 2600, 3600, and 3700 series routers. Each sensor addresses the bandwidth requirements of different routers up to 10 Mbps in the Cisco 2600XM, and up to 45 Mbps in the Cisco 3700 Series. By integrating IDS and branch office routing, Cisco reduces the complexity of securing WAN links and at the same time reduces operational costs. Additionally, by delivering full-featured intrusion protection to remote offices and branch offices, network administrators can now mitigate threats at these remote locations and effectively isolate them from the corporate network. The Network Module has the capability of inspecting GRE/IPsec encrypted packets that are traversing the router into which it integrates.

Q. How does the IDS sensor work?

A. Sensors monitor the network traffic by directly "tapping" the line (for example, via a shared-media hub) or by receiving copies of the traffic (for example, Switched Port Analyzer [SPAN] port on a switch) using a passive, promiscuous interface (the "monitoring interface"). The sensor analyzes the captured packets and compares them against a rule set of typical intrusion activity (that is, "signatures"). If the captured packets match a defined intrusion pattern in the rule set, the sensor sends an alarm to the management console and automatically responds (if configured to do so). The alarms are sent out a separate management interface so as not to impede continual packet capture by the monitoring interface.

Q. What kind of a performance impact does the sensor impose on the monitored network?

A. None. Sensors operate by "tapping" the network (for example, via a shared-media hub) or off copies of the packets (for example, via a switch SPAN port). The monitoring interfaces on the sensors are passive and do not source packets onto the network (the one exception is TCP reset packets for automatic response).

Q. How do you deploy sensors in a switched environment?

A. With most IDS products on the market today, sensors must be placed on the switch SPAN port to monitor network traffic. Although the SPAN port can provide access to network traffic, it does have certain limitations (for example, limited number of SPAN sessions). The Catalyst 6000 IDS Module was designed specifically to address switched environments by integrating the IDS functionality directly into the switch and taking traffic right off the switch backplane.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1099
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. What is the Cisco IDS Network Module for the Cisco 2600, 3600, and 3700 series routers?

A. The Cisco IDS Network Module is a network module that is installed in a Cisco 2600, 3600, or 3700 series chassis to provide full-featured intrusion protection services within the router. The Cisco 2600, 3600, and 3700 Series IDS Network Module provides the ability to inspect all traffic traversing the router, to identify unauthorized or malicious activity such as hacker attacks, worms, or denial-of-service attacks, and to terminate this traffic to suppress or contain threats.

Q. How does the Cisco IDS Network Module work?

A. The Cisco 2600, 3600, and 3700 Series IDS Network Module receives copies of packets directly from the router's backplane in a passive or promiscuous mode. The packets are passed through the internal monitoring interface for classification and processing. The Cisco 2600, 3600, and 3700 Series IDS Network Module analyzes the captured packets and compares them against a rule set of typical intrusion activity. If the captured packets match a defined intrusion pattern in the rule set, the IDS Network Module can take one of two actions. It can send a command to the router to either shut down the interface or it can send a TCP reset packet to the sender to stop the TCP session causing the attack.

Q. What is the rated performance of the Cisco 2600, 3600, and 3700 Series IDS Network Module?

A. The Cisco 2600, 3600, and 3700 Series IDS Network Module provides up to 10 Mbps for the 2600XM Series and up to 45 Mbps for the 3700 Series, depending on the platform in which the network module is inserted.

Q. Can the Cisco Network IDS Sensors monitor trunked traffic?

A. Both IDSM and the appliance sensors can monitior 802.1q traffic and, hence, are VLAN aware.

Q. What type of interfaces are supported on the appliance sensors?

A. Copper interfaces are supported on the IDS 4215 and IDS 4235. Both Copper and Fiber interfaces are supported on the IDS 4250 Sensor. The 4250-XL supports dual fiber interfaces with MTRJ connectors.

Q. Does Cisco IDS provide multi-interface support?

A. Yes. Dual sniffing interfaces are supported on the IDS 4250-XL. Up to 5 interfaces are supported on the IDS 4215, 4235, and 4250 Sensor appliances.

A configurable four Fast Ethernet interface card is provided for other models of the Cisco 4200 Series sensors to deliver a total of five sniffing interfaces for each sensor—one onboard sniffing interface plus four Fast Ethernet configurable interfaces.

The Cisco IDSM-2 can be used to monitor traffic from multiple interfaces. The network module for the Cisco access routers can monitor traffic from any of the router interfaces.

Q. Is the user notified when the sniffing interface of a sensor is disconnected?

A. Sensors are equipped with a monitoring interface for data packet capture and a command and control interface for transmitting alarms to the management console and receiving configuration information from the management console. When the sniffing interface is disconnected, an alarm is triggered. This setup provides the user with an alert mechanism when the interface is tampered with and, hence, assures persistent operation.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1100
3690
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. Does the Cisco IDS Sensor provide an indication of when it is oversubscribed?

A. Yes. The sensor, IDSM, and network module issue an alarm when their respective performance ratings are exceeded.

Q. Where can I find more details on the IDS signature algorithms?

A. For more information on the signature algorithms, please refer to a white paper that may be downloaded at:

http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idssa_wp.htm

Q. Does Cisco IDS protect against common IDS evasion techniques?

A. Cisco IDS also includes protection from a number of advanced, anti-IDS evasion techniques including:

- IP fragmentation reassembly
- TCP streams reassembly
- Unicode Web deobfuscation

Q. Can the sensor itself be attacked and compromised?

A. A properly configured and installed sensor cannot be compromised. The monitoring interface (connected to the production network) cannot be detected, and packets cannot be directed at it. The interface is in promiscuous mode, and has neither a protocol stack nor an IP address bound to it. It is not susceptible to "antisniff" detection techniques. The separate management interface does have an IP address, but Cisco recommends that a separate, isolated management subnet be used to provide connectivity from the management interface on the sensor to the IDS management console. In addition, only a very limited number of services are available from the management interface, and access controls can be configured to allow only designated management systems to connect to the sensor.

Q. What is Cisco Countermeasures Research Team (C-CRT)?

A. The core of the Cisco IDS solution—the advanced protection capabilities—is developed and maintained by C-CRT. This team of elite security professionals is dedicated to:

- Advancing countermeasures research
- Identifying and responding to new threats
- Distributing proactive signature files and signature micro-engines
- Maintaining our network security database (NSDB)
- Contributing research to the Cisco Security Encyclopedia (CSEC)
- Improving the state of threat mitigation science

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1101
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The C-CRT is comprised of elite "white hat" personnel. C-CRT's esteemed credentials include:

- *Heritage and tenure*—most joined Cisco through the WheelGroup acquisition.
- *Government clearance*—greater than 65 percent have held Secret and Top Secret Department of Defense security clearances.
- *Military backgrounds*—experience logged from USAF Information Warfare Center, Department of Defense (DOD), Department of Energy (DOE), National Security Agency (NSA), Central Intelligence Agency (CIA), or other notable government organizations.
- *Security experience*—average member of the C-CRT has over six years of computer security experience, allowing Cisco to deliver the most mature, accurate, and industry-proven intrusion protection solutions.

Q. Can I create my own signatures?

A. Because the security objectives for each IDS deployment are unique, Cisco IDS adds granularity to the way in which sensors may be tuned to specifically suit the environment in which they are deployed. Using our innovative TAME (Threat Analysis Micro Engine) policy language, users can create new policies or modify existing policies to meet their unique security objectives. Since the TAME policies are decoupled from the sensing application, changes can be made without affecting sensor performance or reliability.

Q. Is it possible to record and replay the IP session of the source IP address that triggered an IDS alarm?

A. IP session logging provides extensive logging that is important for system troubleshooting as well as for reconstructing system events before and after attacks. Cisco IDS augments this capability by converting these logs to a standard TCP dump format that allows them to be viewed and replayed using public domain utilities, such as Ethereal and TCPReplay.

Q. Can the sensor detect attacks if the traffic is encrypted, for example IPsecurity (IPsec) or Secure Sockets Layer (SSL)?

A. The Cisco IDS Sensor analyzes both packet header information (context data) and packet data information (content data) to determine if suspicious activity is occurring. Encryption algorithms encrypt the data portion of the packet for confidentiality. Because it can process only what it can "see," the Sensor cannot detect attacks that require inspection of the payload or data fields within a packet. It will, however, still alarm and respond to attacks, which are detected from the unencrypted packet header information. All network-based IDSs suffer this problem. Therefore, in networks carrying encrypted traffic, Sensor placement is critical. To take advantage of their full intrusion-detection capability, the Cisco IDS Sensors should be installed where the traffic has already been decrypted. Otherwise, the Sensor can be placed on an encrypted segment and will detect all but the packet data or payload-based attacks.

Q. What techniques does Cisco use for mitigating threats?

A. Several techniques provide comprehensive protection against the latest cyber threats, including simple pattern matching, stateful pattern matching, protocol anomaly detection, heuristic-based detection, and anomaly detection.

Q. Does Cisco IDS deliver Peer to Peer signatures?

A. Yes. Cisco IDS delivers protection against file-sharing threats with support for advanced P2P attack mitigation techniques.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1102
3690
Doc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. How are the Cisco IDS signatures updated?

A. Cisco posts signature updates on Cisco Connection Online (CCO) approximately every 14 days. Cisco IDS provides a facility to automatically distribute new signature files and application upgrades to sensors without operator involvement. Utilizing a secure staging technique, new signature files are placed on a central server and passed to the sensor at scheduled intervals. After verifying the integrity of the package, the sensor automatically installs the update. This new capability significantly streamlines the process of regularly updating remote sensors, thereby lowering the recurring operational costs associated with this task. Additionally, users can subscribe to Cisco Active Update notification services to stay informed about breaking vulnerability news and posted countermeasures at:

http://www.cisco.com/warp/public/779/largeent/issues/security/idsnws/archive.html

Users may refer to the following site for a chronological listing of the Cisco IDS Active Update Notification Bulletins:

http://www.cisco.com/warp/public/779/largeent/issues/security/idsnws/archive.html

Q. How do the Cisco IDS Sensors and management consoles communicate with each other?

A. Communication between the Cisco IDS 4.0 Sensors and management consoles is provided by a secure (SSL) XML based messaging format. All alarm transmissions from the sensor to the management console are acknowledged.

If connectivity from the sensor to the management console is disrupted, the sensor will continue to monitor the network, and will queue alarms and retransmit until successful.

Q. How much additional network traffic does the Cisco IDS generate?

A. Because each alarm and acknowledgment is contained in a single UDP packet, there is negligible impact on network traffic.

Q. Is there a site that lists all the supported Cisco IDS signatures?

A. Yes. Users may access the latest Cisco IDS signatures at the Cisco Secure Encyclopedia site at:

http://www.cisco.com/pcgi-bin/front.x/csec/idsHome.pl

Q. Does Cisco support a centralized site that contains a compiled listing of the latest vulnerabilities?

A. Yes. Cisco's Security Encyclopedia is a one-of-a-kind clearinghouse of security and vulnerability information. Unlike other security databases that simply consolidate vulnerability information published on a number of public-source Web sites, the CSEC contains statistics on the vulnerabilities by industry or by sector. These statistics are compiled from over 400 actual Security Posture Assessments (SPA) performed by the Cisco Security Consulting team. CSEC is developed and maintained by the elite C-CRT. You may visit the CSEC site at:

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

Q. Where can I download the latest IDS software?

A. Both current and archived IDS Sensor software can be downloaded at the Software Center on CCO (CCO login required):

http://www.cisco.com/public/sw-center/ciscosecure/ids/crypto/

Q. Where can I access documentation on the Cisco IDS Sensor Software?

A. Documentation for sensor software updates are available at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1103
Fls. Nº
3690
Doc:

Threat Response Technology

Q. Is Threat Response an event correlator?

A. Threat Response is not an event correlator. Event correlation involves analyzing data from NIDS sensor, firewalls, routers, and other sources. Instead of correlating this type of data, Threat Response investigates the actual target of an attack. This is the same process an expert network security specialist would use, and is the best way to determine if a system has been compromised.

Q. Does Threat Response conduct network vulnerability scans?

A. No, Threat Response does not conduct enterprise wide scans of your environment, nor does Threat Response inventory your network. The designers of Threat Response have been network administrators for large mission-critical enterprises such as the U.S. Pentagon and know that downtime is unacceptable. Because of this, Threat Response conducts a low-impact investigation of targeted systems only when needed. Threat Response is able to work in dynamic network environments (including DHCP and wireless) without the need to run regular vulnerability scans that can disrupt your enterprise.

Q. Does Threat Response require deployment of software across the enterprise?

A. No, Threat Response does not require the deployment of software across the enterprise. Threat Response accesses these systems in the same way a security network administrator would—with read access privileges.

Q. How does Threat Response stay up to date with the latest attacks?

A. Cisco releases updates to keep the Threat Response IDS signature database up to date with the IDS vendors, as well as corresponding forensic signature updates to investigate IDS events. When an update is available, the administrator will be notified via the Threat Response GUI and can use the integrated auto-update feature to keep the product current.

Q. What does Threat Response do once real attacks are identified?

A. Threat Response will provide the user with detailed information on how the event was investigated, as well as any forensic data gathered showing details on the actual attack. This information can then be used by an administrator to quickly remediate an intrusion.

Q. What type of systems can Threat Response investigate?

A. Threat Response can conduct a full active investigation of systems running Windows-based operating systems. For systems running Linux, Solaris, and other forms of UNIX, Threat Response will perform passive checks as a first line of investigation. Based on this initial analysis, Threat Response can eliminate many alarms that are not targeted to those specific platform types.

Q. How do I get Threat Response technology?

A. Threat Response technology is currently available as a full featured, 90-day free trial software solution. The trial version ships with every Cisco IDS sensor. Once the trial has expired, customers have the choice of:

- switching to a reduced capabilities free version (only conducts basic level investigation of the targeted system)
- purchasing the full featured version, which will be offered as part of a VMS bundle

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1104
Doc. 3690

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Management

Q. What management console options are available for the Cisco IDS?

A. See Table 1 and Table 2.

Table 1 Event Management

	IEV	IEV with CTR Technology	VMS SecMon	VMS SecMon with CTR Technology
Deployment method	Dedicated system required	Dedicated system required	Dedicated system required	Dedicated system required
GUI type	Java desktop application	Browser-based GUI	Browser-based GUI	Browser-based GUI
# sensors	5	5	Unlimited	Unlimited
Event types	IDS	IDS	IDS, Firewall, Router	IDS, Firewall, Router

Table 2 Device Management

	IDM	CLI	VMS Management Center
Deployment method	Integrated on sensor	Integrated on sensor	Dedicated system required
GUI type	Browser-based GUI	Browser-based GUI	Browser-based GUI
# sensors	Unlimited, by sensor	Unlimited, by sensor	Unlimited, by sensor groups
Event types	IDS	IDS	IDS, Firewall, Router

IEV = Cisco IDS Event Viewer, included free of charge with IDS sensor
VMS SecMon = CiscoWorks Monitoring Center for IDS, part of the CiscoWorks VMS bundle
IDM = IDS Device Manager, included free of charge with the IDS sensor
CLI = Command-line interface, included free of charge with the IDS sensor
VMS Mgmt Center = CiscoWorks Management Center for IDS, part of the CiscoWorks VMS bundle

For More Information

More information on Cisco's VMS solutions can be found at:

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

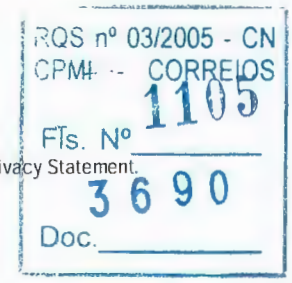
In addition, augmentation to the alarm viewing, analysis, and reporting capabilities of the Cisco IDS Management solution are provided through third-party applications that are available from Cisco Security Associates partners.

For more details see:

http://www.cisco.com/warp/public/778/security/sap/management.html

Q. Are Cisco IDS communications encrypted?

A. IPsec functionality is included on the appliance Sensors to allow customers to encrypt traffic to management consoles with IPsec capabilities.



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. If I lose connectivity to a remote sensor, can I tell from the management console?

A. The Cisco IDS management consoles monitor the health of a Sensor via a continuous heartbeat. If communications with the Sensor are lost for more than one minute (by default), a visual indicator is displayed on the management console, indicating a communications failure with the Sensor. If it is determined that a sensor has failed, it can be quickly replaced with another sensor and the configuration, stored on the management console, and can be quickly pushed to the new sensor.

Q. How many sensors can one Cisco IDS Management console manage?

A. Although the technical limit is very large (greater than 1000), Cisco typically recommends a ratio of 20 to 25 sensors per management console for practical reasons. With ratios greater than this, operators can be easily overwhelmed with the volume of information that they may be required to analyze, thereby diminishing the overall effectiveness of the IDS. For deployments larger than 25 sensors, multiple management consoles can be installed to scale the number of sensors.

Q. Can I have multiple Cisco IDS management consoles?

A. The Cisco IDS architecture supports the deployment of multiple management platforms. Sensors can send alarms to multiple management consoles simultaneously, and management consoles can forward alarms to other management consoles, allowing customers to build large, hierarchical management infrastructures.

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW4425 05/03

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1106
Doc. 6 9 0

E C T
160
CPL - AC

Intrusão doc 5

RQS nº 03/2005 - CN
CPMI - CORREIOS
1107
Fls. Nº
3690 -
Doc.

Data Sheet

Cisco **Intrusion Detection** System **Management Solutions**

Introduction

The Cisco Intrusion Detection System (IDS) is designed to address the increased requirements for intrusion protection for networks.

Cisco Network IDS solutions have two components: the Cisco IDS Sensor and the Cisco IDS Management Console. Cisco IDS provides the user with unparalleled flexibility by delivering the industry's broadest breadth of management solutions to remotely monitor, configure, and manage Cisco IDS sensors. The three-tiered Cisco IDS management solutions include:

- Highly scalable Cisco VPN and Security Management solutions (VMS)
- Integrated Web user interface: IDS Device Manager
- Command-line interface (CLI)

Each solution delivers ease of use, scalability, performance, and reliability required for enterprise and service provider networks.

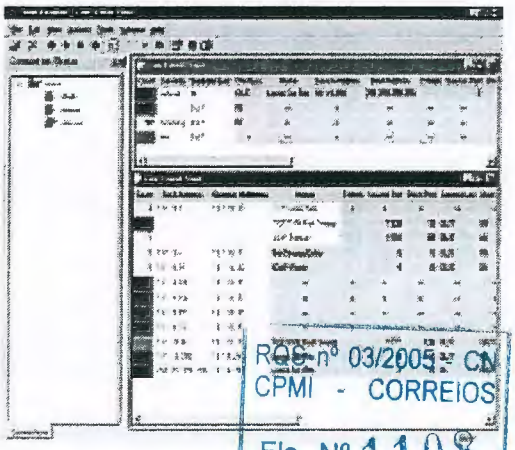
CiscoWorks VMS

CiscoWorks VMS is a software-based enterprise management solution suite that provides a comprehensive solution for VPN and security management. Cisco VMS is used for configuring, monitoring, and troubleshooting enterprise virtual private networks (VPNs), firewalls, and network- and host-based intrusion detection systems. This scalable solution addresses the needs of small- and large-scale VPN and security deployments.

Cisco Secure Policy Manager, a component of CiscoWorks VMS, is a scalable, powerful, policy-based security management system for Cisco PIX® Firewalls, IP Security (IPSec) VPN routers, and Cisco IDS sensors. Cisco Secure Policy Manager can centrally configure and monitor the activity of multiple Cisco IDS sensors located on local or remote network segments.

Cisco Secure Policy Manager allows network and security technicians to quickly pinpoint the location and type of an attack, qualify its severity, and instantly respond. Cisco Secure Policy Manager Event Viewer provides the user with unmatched ability to filter through large volumes of alarms in real time. The attributes used to define the way in which alarms are viewed on the event viewer may also be used to define a variety of HTML-based reports. For smaller operations that will not employ 24 x 7 operations, Cisco Secure Policy Manager can be easily instructed to forward alarms to a paging system and e-mail to help track events to resolution. Cisco Secure Policy Manager can also configure the Cisco IDS Sensor to perform response actions upon the firing of an alarm. These response actions include shunning on routers, firewalls, and switches; TCP resets; and, IP session logging.

CSPM Event Viewer:
Ability to easily manage IDS alarms in real time utilizing an intuitive and highly scalable tabular format



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1108
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Features and Benefits

- *Multidevice management and monitoring*—Cisco IDS offers management support for Cisco IDS sensors, Cisco PIX firewalls, and Cisco VPN.
- *Centralized configuration management*—Cisco Secure Policy Manager can manage sensor configuration. Cisco Secure Policy Manager allows the user to easily and remotely fine-tune a variety of configuration parameters. In addition, a variety of proactive response actions may be configured on the Cisco Secure Policy Manager console on a per-signature basis; these actions enable the user to terminate sessions upon signature triggering. Such response actions include TCP resests, shunning (or blocking), and IP session logging.
- *Highly scalable event viewer*—The Cisco IDS Event Viewer (IEV) provides unparalleled scalability by enabling the user to view and easily perform complex data mining for large volumes of alarms, thereby keeping network administrators readily informed of network-wide events. Filtering of events may be easily accomplished on a wide range of attributes. Multiple instances on the event viewer allow the user to concurrently view the data in numerous different perspectives.
- *E-mail notification and script execution*—Cisco Secure Policy Manager sends e-mail notifications to a pager or a user account when alarms are received. In addition to the use of example scripts provided by Cisco IDS sensors, custom scripts can be easily created for notification purposes.
- *Secure communication*—IPSec can be configured to provide secure encrypted communication between the Cisco Secure Policy Manager and the Cisco IDS Sensor.
- *Reporting*—Reporting allows the creation and viewing of reports about network activities monitored by sensors on your network. The reports include summary reports based on alarms, sources, destinations, or a specific sensor on your network. Because these reports are HTML based, they can be sent via e-mail to key administration personnel.
- *Network security database*—The system network security database (NSDB) provides a technician instant access to specific information about the attacks, hotlinks, potential countermeasures, and related vulnerabilities. Because the NSDB is an HTML database, it can be personalized for each user to include operation-specific information such as response and escalation procedures for specific attacks.
- *Windows NT-based system*—The system provides an easy-to-use, Windows-based user interface.

System Requirements

Recommended Platform

- Microsoft Windows NT Server 4.0 with Service Pack 6a*
- Microsoft Internet Explorer 5.5 or above
- Intel-based Pentium II processor, 400 MHz or better
- 128 MB RAM
- 4 GB of free hard drive space available
- One or more properly configured network adapters ·Video display-1024 x 768, with 64K color support
- CD-ROM and 3.5-in. diskette drive

* If installed in a distributed mode, the Cisco Secure Policy Manager graphical user interface (GUI) can also run on Microsoft Windows 95, 98, 2000, and NT 4.0. Demo mode is also supported on Windows 2000 in Cisco Secure Policy Manager 2.3.

Ordering Information

Table 1 gives ordering information for components of the Cisco IDS management system.

Table 1: Ordering Information for Cisco IDS Components

Part Number	Description
CWVMS-2.0-WINR-K9	Cisco VMS bundle (includes Cisco Secure Policy Manager [ten devices] and host console)
CWVMS-2.0UR-K9	Cisco VMS bundle (includes Cisco Secure Policy Manager [unrestricted] and host console)
CON-SAS-CWVMS-R2	Software Application Services for VMS 2.0 (restricted)
CON-SAS-CWVMS-UR2	Software Application Services for VMS 2.0 (unrestricted)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1109
Doc. 3695

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

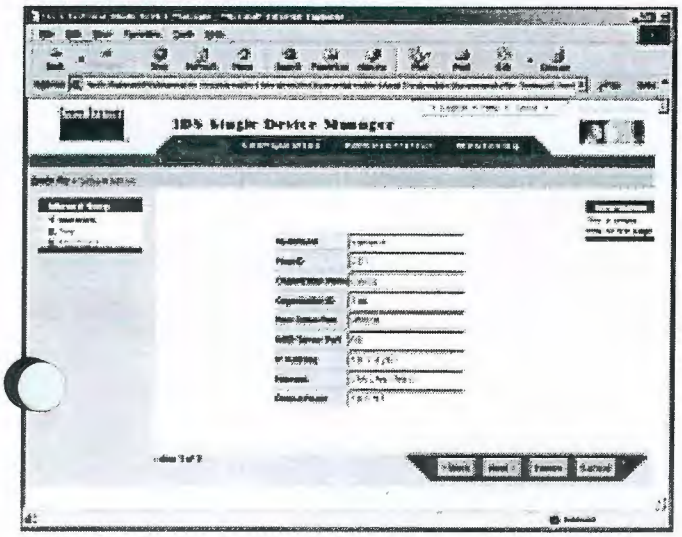
Cisco IDS Device Manager and IDS Event Viewer

Cisco IDS 3.1 Sensor Software delivers Web-based embedded device management with the Cisco IDS Device Manager (IDM) and Cisco IDS alarm monitoring capabilities with the Cisco IEV. Cisco IDS 3.1 ships with the Cisco IDS Appliance Sensor, and provides powerful and easy-to-use management capabilities using a cost-effective approach.

Through the use of simple, intuitive, Web-based graphics, Cisco IDM enables the easy configuration of a Cisco IDS Sensor without requiring CLI knowledge. The Cisco IDM user interface supports wizard-based IDS command sets and a point-and-click design that allows unprecedented ease of configuration in just a few steps, resulting in reduced deployment time. The result is cost savings through significant reductions in management time and maximum efficiency in Cisco IDS Sensor management.

Cisco IDM provides secure communications by utilizing the Secure Sockets Layer (SSL) protocol to provide high-grade encryption for configuration of the Cisco IDS Sensor. The embedded design of Cisco IDM also enables management from practically any desktop using a Web browser, providing operational convenience to all deployment environments.

IDS Device Manager (IDM):
Enterprise-class, web-based management, providing wizards-based configuration for ease of use, including instruction panels to guide the user through every step of the configuration.



Cisco IEV is the component of Cisco IDS 3.1 Sensor software that delivers powerful centralized event monitoring functionality for Cisco IDS sensors. The Cisco IEV is a Java-based application that enables users to view and manage alarms from up to three sensors.

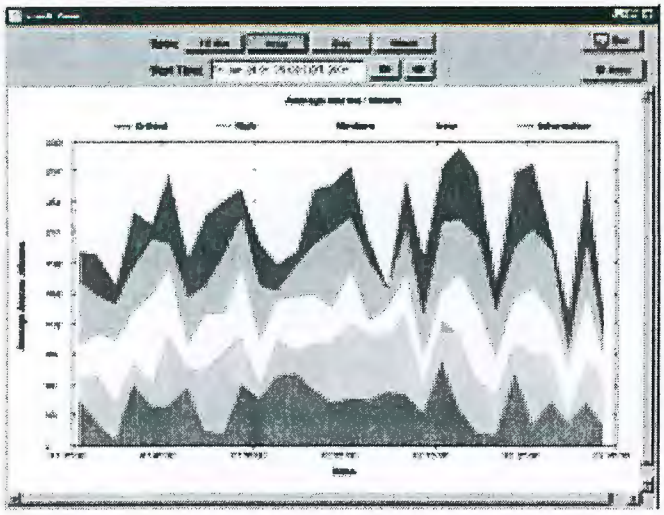
Features and Benefits

- *Embedded architecture*—The embedded design of Cisco IDM allows customers to manage their Cisco IDS appliance sensors from practically any desktop, no matter which operating system is being used on the desktop. Authorized administrators can securely point their Web browser at the Cisco IDS Sensor for deploying configurations. Cisco IDM provides support for the most popular browsers in the market today, including Microsoft Internet Explorer and Netscape Navigator.
- *Wizard-based configuration management*—The feature provides wizards to guide the user through the configuration process, allowing sensors to be configured quickly and easily.
- *Graphical User Interface (GUI)*—The interface delivers a tabular layout with one-click access to common tasks, enabling even the novice user to easily configure sensors using its point-and-click design. Furthermore, instruction panels describe the individual GUI screens in detail. After the initial configuration is complete using default configuration parameters, intuitive pull-down menus and dialog boxes are provided for users who wish to tune their sensors at a granular level to customize the configuration to address specific threats that are applicable to their environment.
- *Granular level of signature configuration*—Cisco IDM allows the assignment of severity levels, disabling and enabling of signatures, and the configuration of response actions, such as shunning, TCP resets, and IP session logging, at a per-signature level.
- *Signature group*—Cisco IDM groups signatures into logical categories based on the type of attack to which they pertain. This enables users to specify configurations globally to all signatures contained in the particular signature group.
- *Signature customization*—Cisco IDM is fully compatible with the Cisco Signature Micro-Engine (SME), which enables the user to easily create custom signatures and tune existing signatures. The result is sensors that are fine-tuned to specifically address the security environment in which they are deployed, thereby minimizing the occurrence of "false positives."
- *Highly scalable event viewer*—Cisco IEV provides flexibility in event viewing by allowing the user to toggle between an innovative graphical representation of the alarms and a highly scalable and intuitive tabular format. A combination of these techniques allows users to drill down and view event information at a granular level and also select a variety of attributes with which to filter alarms, hence providing an unprecedented approach to alarm management and data mining.

ECT
SCI
EOS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1110
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Cisco IDS Event Viewer (IEV):
Delivers innovative graphical display of IDS alarms



- Secure communication—Secure Socket Layer (SSL) encryption secures the communication between the Cisco IDS Sensor and the browser.
- *Scalable event storage database*—Cisco IEV delivers a robust, high-performance database that ensures high data insertion rates to deliver persistence, and provides ample data storage capacity for scalability.
- *Network Security Database (NSDB)*—The NSDB is an HTML database that provides detailed descriptions of attacks and recommendations for countermeasures.

Network Security Database (NSDB):
Online reference tool that provides detailed description about attackes, potential countermeasures, and links to available patches.

System Requirements for Cisco IDM and Cisco IEV

Recommended Web Browser (Cisco IDM)

- Netscape (Version 4.5 or higher)
- Internet Explorer (Version 5.01 Service Pack 1 or higher)

Recommended Platform (Cisco IEV)

- Intel-based Pentium III, 600 Mhz or greater.
- 128 MB RAM
- 500 MB of free hard drive space available
- Video display-1024 x 768, with 64K color support
- CD-ROM drive
- Windows 2000 Professional and Server

Ordering Information for Cisco IDM and Cisco IEV

Cisco SMARTnet® customers may download Cisco IDS 3.1 from the Software Center on Cisco.com at http://www.cisco.com.

The part number for Cisco IDS Software Upgrade for customers who do not have Cisco SMARTnet support is IDS-SW-U.

Additional Information

For more information about Cisco IDS, go to:
http://www.cisco.com/go/ids.

For more information on Cisco VMS Solutions go to:
http://www.cisco.com/go/vms

RQS nº 03/2005 - CN
CPMI - CORREIOS
1111
Fls. Nº
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT
Local
COL - AC

CISCO SYSTEMS

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

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

ECT nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1112
Doc 3690

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

E C T
AC

Intrusão doc 6

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1113
Doc 3690

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

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1114
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

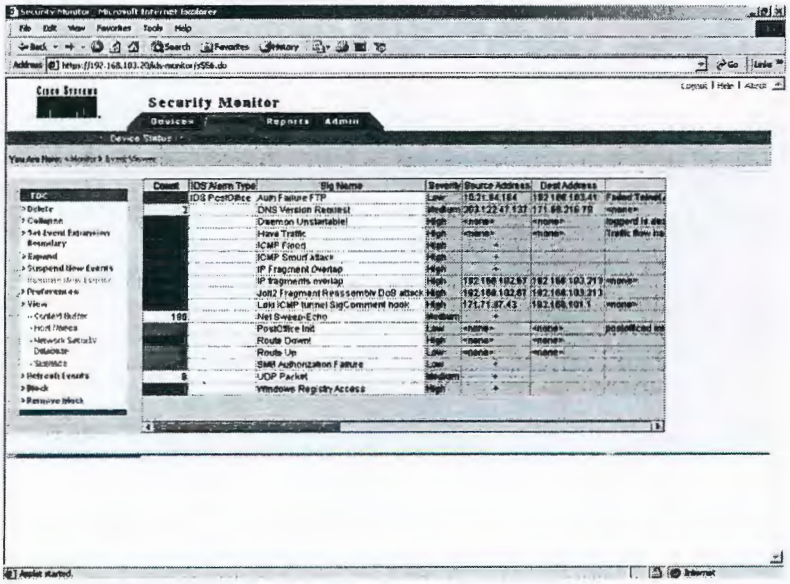
Web-based event viewer with features to easily locate attacks

- 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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1115
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 116
Doc. 6 9 0 -

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 111
3690
Doc.

I E C S
C P L - A C

Intrusão doc 7

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1118
3690
Doc.

Cisco **IDS 3.0** Sensor Software for Cisco 4200 Series Appliances

The industry-leading Cisco IDS Intrusion Detection System solution provides customers with unmatched intrusion protection technology through the Cisco Active Defense System. The integrated hardware and software solution delivers best-of-breed protection for both perimeter and internal resources.

Version 3.0 is the latest release of the Cisco IDS application software for the Cisco 4200 Series appliances. It delivers the latest in innovative IDS features, including Active Update signature distribution mechanisms, customizable signature language, extensions to the Active Response capabilities, and secure administration.

Key Features and Benefits

Signature Definition and Distribution Enhancements

Active Update Mechanism

Cisco IDS now 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.

Signature Instruction Language for Verifying Exploits and Reconnaissance (SILVER)

Cisco IDS continues to innovate with the release of the Cisco SILVER signature language. Users can now develop custom signatures spanning Layer 2 through Layer 7 attributes. Developed by the Cisco Countermeasures Research Team, SILVER is the mechanism that this team uses to develop all new signatures for the IDS product. Now Cisco is exposing this capability to its customers, providing them unparalleled flexibility to develop new signatures.

This new language also decreases the time between signature releases because the signatures can be released as update files rather than compiled in the core sensor binary. Similar to antivirus products, the signature engines and the data files can be released separately.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1119
Doc 90

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Tunable Signatures

One of the challenges of event monitoring for IDS is to reduce the occurrence of false positives, thereby allowing the user to focus only on alarms that are deemed security relevant. However, because the security objectives for each IDS deployment are unique, Cisco IDS 3.0 adds granularity to the way in which sensors may be tuned to specifically suit the environment in which they are deployed. Users may now tune signature threshold parameters to meet their unique security objectives. For example, for the ping sweep signature, the user can now define the number of hosts pinged before the signature fires.

Alarm Summarization

Attackers may use tools such as Stick to cause sensors to send numerous alarms to management consoles as a way of flooding the management console. The Alarm Throttle feature in Cisco IDS 3.0 allows users to consolidate alarms to a single event, thereby preventing the management console from being overwhelmed with numerous events. For example, if the rate of alarms being sent by the sensor exceeds a certain threshold value, the signature may be set to automatically throttle to a summarization mode to produce a single alarm that comprises numerous alarm firings. A time interval may also be specified that determines the rate at which subsequent consolidated alarms are sent to the management console.

Detection of Network DoS Attacks

Cisco IDS 3.0 adds functionality to detect network denial-of-service (DoS) attacks that are targeted at consuming network resources. An inspector monitors the data capture by maintaining a counter that tracks the number of packets being captured per second. If the rate of packets being captured exceeds a specified rate and such peaks occur at a certain frequency, an alarm is generated to alert the user of a possible DoS attempt.

Active Response Extensions

Shunning with the Cisco PIX Firewall and Cisco Catalyst Switches

Cisco IDS incorporates proactive response functionality into the sensor appliances by allowing users to configure the IDS to dynamically respond to an attacking host by preventing new connections and disallowing packets from any existing connection. Cisco IDS 3.0 extends this Active Response capability beyond Cisco routers into a wide range of Cisco's high-performance networking devices, including the Cisco PIX® Firewall (running PIX 6.0+), Cisco Catalyst® 6000 Switch, and Cisco Catalyst 5000 Switch. This shunning gives security operators unparalleled control to reach across the network to quickly stop misuse and end intruders' access to the network.

Interoperability with Existing ACLs

Shunning is accomplished by the dynamic modification of access control lists (ACLs) on managed devices. Cisco IDS 3.0 allows the user to configure the sensor to shun while maintaining any user-defined access control entries on the specified interface and direction.

Secure Administration

In addition to existing functionality that provides secure communications between the sensor and the management console using IP Security (IPSec), Cisco IDS 3.0 also supports the Secure Shell Protocol (SSH) to allow users to remotely access sensors over a secure connection.

IP Session Replay

IP session logging provides extensive logging that is important for system troubleshooting as well as for reconstructing system events before and after attacks. Cisco IDS 3.0 augments this existing capability by converting these logs to a standard TCP dump format that allows them to be viewed and replayed using public domain utilities, such as Ethereal and TCPReplay.

Enhanced Filtering

Users have the ability to specify which source or destination IP addresses that specified signatures must alarm on. Because certain signatures may be classified as security relevant for certain source or destination IP addresses and yet do not need to be analyzed for other IP addresses, this level of enhanced filtering minimizes the occurrence of false positives.

Alarm Generation When Sniffing Interface is Disconnected

Sensors are equipped with a monitoring interface for data packet capture and a command and control interface for transmitting alarms to the management console and receiving configuration information from the

ROS nº 03/2005 - CN
CPMI - CORREIOS
1120
Fls. Nº
5690
Doc.

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

management console. With Cisco IDS 3.0, when the sniffing interface is disconnected, an alarm is triggered. This setup provides the user with an alert mechanism when the interface is tampered with and hence assures persistent operation.

Technical Specifications

Ordering Information

SMARTnet™ customers may download Cisco IDS 3.0 from Software Center on CCO at http://www.cisco.com

Part number for IDS Software Upgrade for Non-Support Customers: IDS-SW-U

Export Considerations

IDS sensors are subject to export controls. Please refer to the export compliance Web site at

http://www.cisco.com/wwl/export/crypto/ for guidance.

For specific export questions, please contact export@cisco.com.

Additional Information

Cisco Secure Intrusion Detection System:

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

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

European Headquarters
Cisco Systems 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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. SMARTnet is a trademark of Cisco Systems, Inc.; and Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

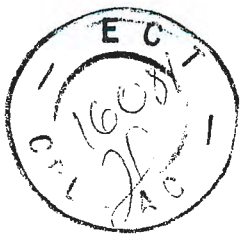
All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

Printed in the USA

LW2654 09/01

ECT 16 CSL CPL AC

BOLSA 03/2005 CN CPMI - CORREIOS FLS. Nº 1121 3690 Doc.



Intrusão doc 8

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº
1122
Doc 3690

Tuning Sensor Configurations

After configuring your sensors, you need to 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 signature parameters.

Some legitimate network activity, such as virus scanning, can appear to be an attack on your network. When legitimate network activity is reported as an attack, that report is called a *false positive*. More generally, a false positive can be defined as the interpretation of an instance of legitimate and expected network activity as an attack because that activity meets criteria that were specified to identify an attack prior to the occurrence of the attack. You can decrease the number of false positives by tuning your sensor configurations.

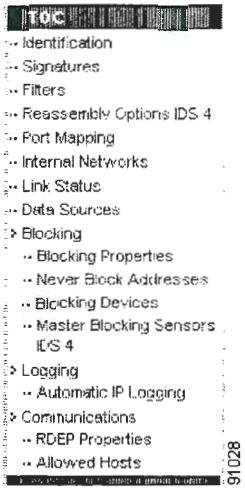
Tuning your sensor configurations can also help you solve another problem. You can decrease the number of *false negatives* by tuning your sensor configurations. A false negative can be defined as an attack that was not detected.

You can tune sensor configurations by using four general methods:

- Specifying *reassembly settings* for IP fragments and TCP sessions.
- Port mapping (that is, identifying additional ports).
- Identifying hosts and networks that should be exempt from *blocking*.
- *Filtering* alarms in accordance with their severity and their source.

CPMI - CORREIOS
Fls. Nº 1123
Doc 3690

Reassembly Options, Port Mapping, Never Block Addresses, and Filtering are in the TOC that appears when you select Configure > Settings in IDS MC.



You can tune sensor configurations by specifying reassembly options for IP fragments and TCP sessions. Specifying reassembly options prevents false negatives that are caused because the sensor cannot reconstruct the datagram or session.

When using IDSM devices supported by IDS MC, you can identify additional ports that should be considered by a sensor signature. This process is known as port mapping. Examples of these additional ports are those used by custom TCP services and those used by well-known services that you have reassigned to another port. Identifying additional ports is important because some sensor signatures are based on specific port numbers.

You can tune sensor configurations by identifying hosts and networks that should be exempt from blocking.

For example, your sensor configuration may include instructions to block sources of a particular attack whenever that attack is detected; you may also have a trusted network device whose normal, expected behavior appears to be that attack. (This situation results in a false positive.) In this situation, you can tune your sensor configuration to ignore that particular perceived attack when its source is your trusted network device. In that way, you avoid false positives: You avoid the generation of alarms from your trusted network device, and your trusted network

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1124
Doc: 3690

device is not blocked. You still receive alarms if that particular attack is detected in traffic from other sources. Also, you can still block other, untrusted devices if your sensor detects that particular attack in traffic from those other, untrusted devices.

You can tune sensor configurations by filtering audit events. Tuning a sensor by filtering audit events reduces the number of false positives. You can set the minimum level of events that will be reported to you. Also, you can enable and disable alarms from specific hosts and networks.

When using IDSM devices supported by IDS MC, you can define rules that prevent the sensor from generating alarms and audit event records for suspicious behavior based on traffic originating from or destined to specific networks and hosts. You can use the Filters page to define these rules.

Task List for Tuning Sensor Configurations

After configuring your sensors, you need to tune them. You can tune sensor configurations by using four general methods:

- Specifying *reassembly options* for IP fragments and TCP sessions.
- Port mapping (that is, by identifying additional ports).
- Identifying hosts and networks that should be exempt from *blocking*.
- *Filtering* alarms in accordance with their severity and their source.

You can tune sensor configurations by performing one of the following tasks. For step-by-step procedures on performing a specific task, refer to the corresponding section.

- Specifying IP Fragment and TCP Session Reassembly Settings for a Sensor, page 7-4
- Identifying Additional Ports Used by Specific Signatures Applied to a Sensor, page 7-5
- Defining Filters for a Sensor, page 7-7
- Specifying Networks and Hosts that Should Never Be Blocked, page 7-13

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1125
3690
Doc:

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1126
3690
Doc:

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**.

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.

ROS 09/03/2005 CN - CPMI - CORREIOS 1127 Fls. Nº 3690 Doc.

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**.

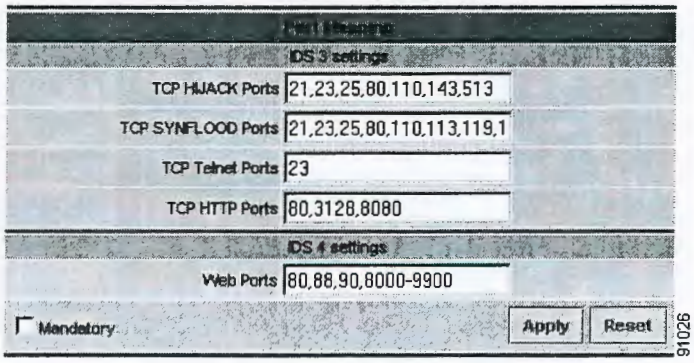
Step 2 Click the **Object Selector** handle.

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1128
3690
Doc:

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**.

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).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1129
Doc. 3690

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.

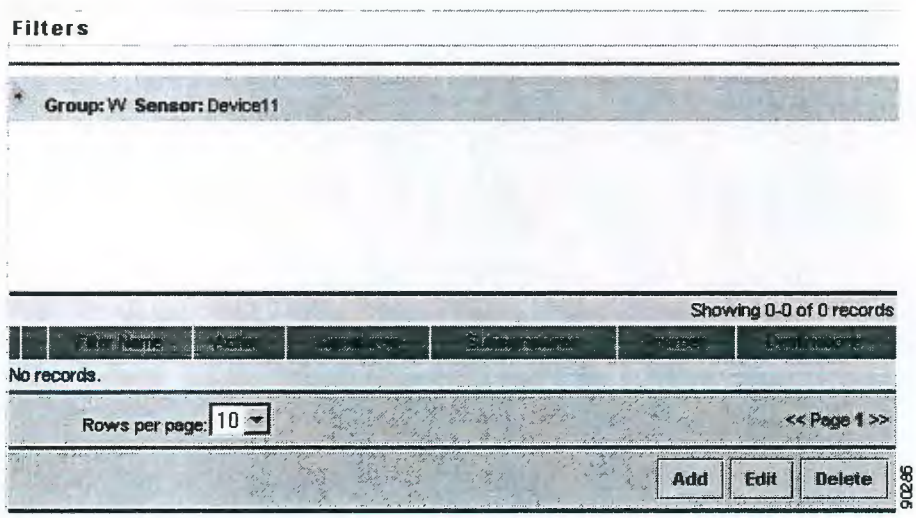
Step 3 In the Object Selector, select Device11, the sensor for which you want to define a filter in this example. Device11 is a 4.x sensor.

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1130
Fls. Nº
3690
Doc:



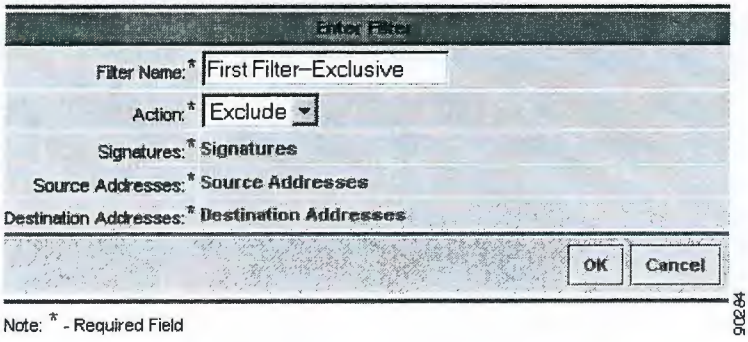
Step 5 To begin defining the exclusive filter in this example, click **Add**.

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.



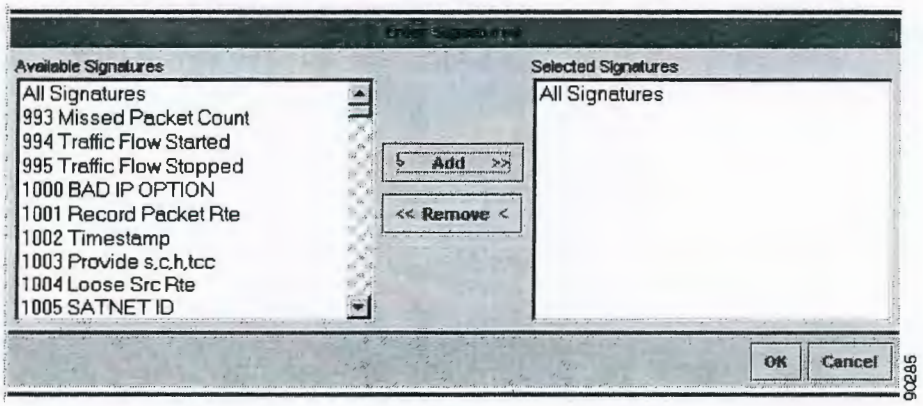
Step 8 Click the **Signatures** link.

The Enter Signatures page appears.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1131
Doc: 3690

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.

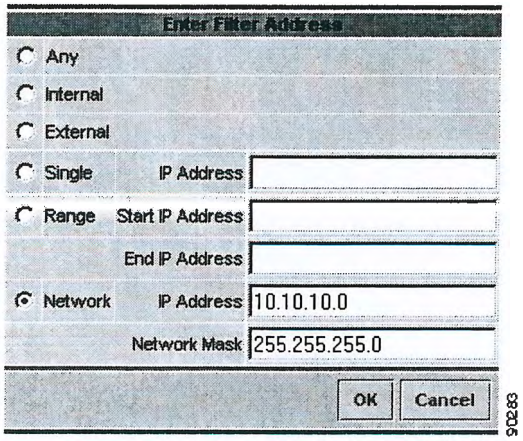
The Filter Source Addresses page appears.

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1132
Doc. 3690



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.

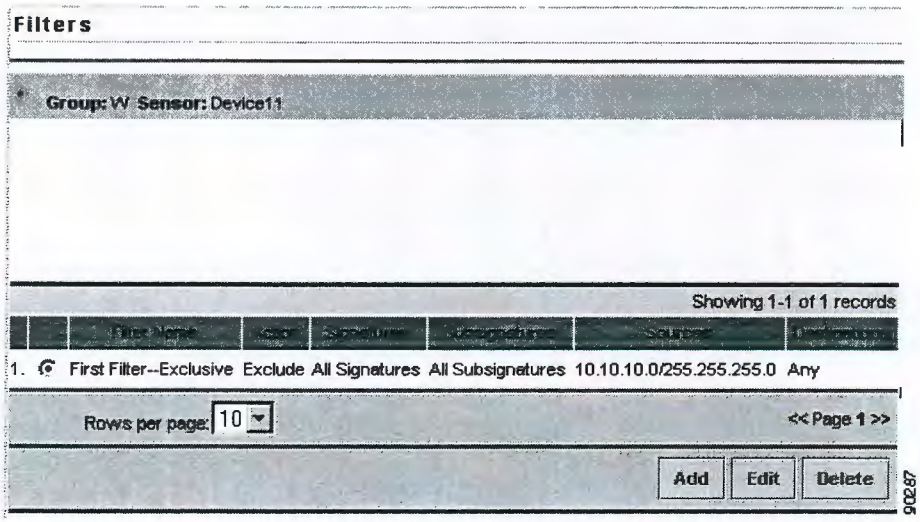
Step 20 Click **OK**.

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.

CEMI - CORREIOS
Fls. Nº 1133
Doc: 3690

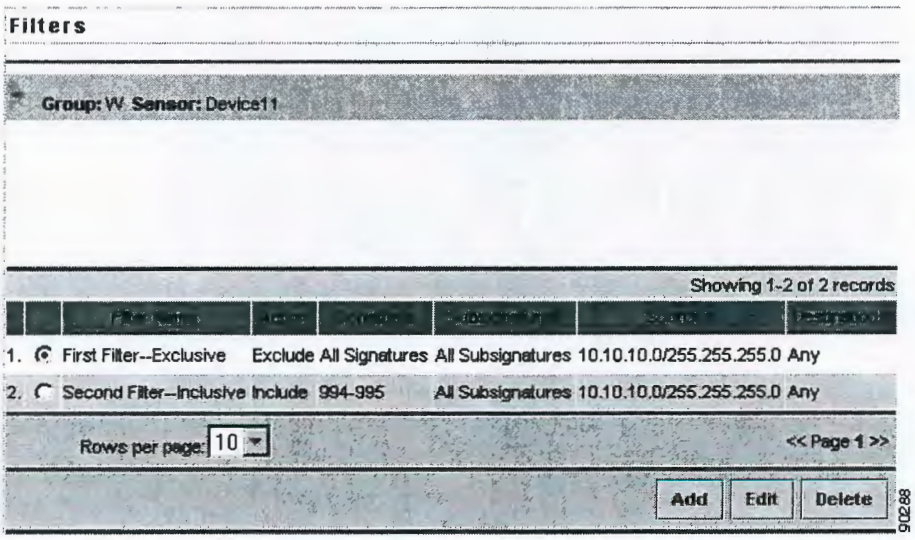


Step 22 To begin defining the inclusive filter in this example, click **Add**.

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 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.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1135
3690
Doc:

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

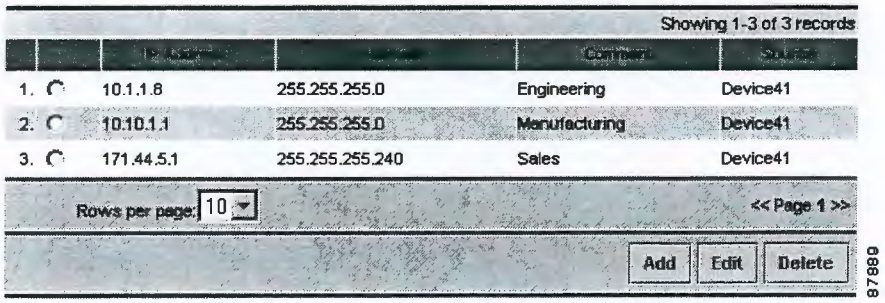
Step 1 Select **Configuration > Settings**.

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.

78-15664-01
CPMI - CORREIOS
1136
Fls Nº
Doc 3690

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**.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1137
Doc: 3690

78-15664-01
ECT 03 2005 - CN -
CPMI - CORREIOS
Fls: Nº 1138
3690
Doc.

Intrusão doc 9

Cisco Systems

Q & A

Monitoring Center for **Security** 1.2

Q. What is The Monitoring Center for Security?

A. It is the next generation event monitoring software from Cisco. The Monitoring Center for Security can view events from:

- Cisco Network IDS
- Cisco Switch IDS
- Cisco IDS Network Module for Routers
- Cisco Security Agents
- Cisco IDS Host Sensors
- Cisco PIX Firewalls
- Cisco IOS Routers

The Monitoring Center for Security will capture, store and provide viewing for these events. Reporting templates are also supplied.

The Management Center for Security is available within the CiscoWorks VPN/ Security Management Solution (VMS). It is not sold separately.

Q. What is additionally required to receive Cisco Security Agent, version 4.0 events?

A. The Management Center for Cisco Security Agents, version 4.0 needs to be installed. This software will forward the events to the Monitoring Center for Security.

Q. Who should buy VMS?

A.

- For larger deployments in enterprises, VMS, which includes the Monitoring Center for Security, would be appropriate. The Monitoring Center for Security also monitors other devices in the Cisco SAFE blueprint, unlike IDS Event Viewer (IEV)
- For monitoring of 1-3 IDS sensors, customers should consider IEV. This is suitable for smaller implementations or trials.
- For those needing high-end scalability and multivendor device support, the CiscoWorks Security Information Management Solution, based on the netForensics version 3.1 technology, would be most appropriate.

Q. How many authorization roles are supported?

A. The software will have five authorization roles. Integration with Cisco Access Control Server (ACS) is also supported for additional user roles.

Q. Does the software require HP OpenView as a prerequisite?

A. The software does not require HP OpenView.

Q. What operating systems are supported?

A. The Monitoring Center for Security, version 1.2 is available for Windows 2000 only. For those requiring Solaris support, the Monitoring Center for Security, version 1.1 is now supported on Solaris 8. However, not all the features that are available on the Windows 2000 supported version, are available on the Solaris supported version. Examples of features not supported on the Solaris platform include:

ECT AC

ECT/ECT - 05/2005 - CN -
CPM - CORREIOS
Fls. Nº 1140
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- 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

Refer to the Cisco web site for availability of the Monitoring Center for Security, version 1.2, with Solaris support.

Note: these components are not available on Windows NT or HP Unix.

Q. For customers with Cisco Secure Policy Manager (CSPM) or IDS Director, what are the advantages to upgrading to the next generation software?

A. Cisco has historically sold two Network IDS management products:

- CSPM for IDS (NT)
- IDS Director (HP Unix and Solaris)

To deal with the increasing adoption of IDS, Cisco developed the Management Center for IDS Sensors and the Monitoring Center for Security. This is an evolution from CSPM and IDS Director.

The aim of the new software is to reduce the effort required for IDS sensor administration. The primary cost for IDS over a three-year period, is not in the hardware or software, it's in the administrative costs. This is where the new features will make the biggest impact. The new software delivers enhancements in several areas to provide lower cost of ownership for IDS management and security monitoring.

1. Higher scalability, supporting deployments to hundreds of sensors
2. Support for higher event volumes
3. Use of group profiles to configure multiple sensors concurrently
4. Event correlation to identify attacks mounted across sensors, across time, and from different addresses
5. Flexible notification scheme to fine-tune what information is sent with each notification and automated responses to critical events.
6. Richer reporting and support for multiple event types
7. More powerful signature tuning to reduce false positives and increase the accuracy of detection
8. Easier web based interface

Existing users will have the option to migrate to the new software through discounted upgrade part numbers. Read the VMS product bulletin for part numbers. Furthermore those customers that have purchased VMS 2.x and a SAS service contract will receive the new software at no additional cost.

Q. Will the software support SNMP alarms?

A. SNMP alarms are currently not supported however this is planned for a future release. The user may consider the use of unsupported freeware tools that generate SNMP traps (e.g. TrapGen). *The Monitoring Center* allows automated scripts to be executed when a specific threshold is exceeded or event type is received. Using the script, the freeware tools can be launched to generate a SNMP alarm. This SNMP alarm can then be forwarded to a third party management console.

Q. Where can I find further information?

A. Refer to the Cisco web site for the latest product and ordering information- http://www.cisco.com/go/vms

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1141
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT
CPL - AC

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202970/ETMG 9/02

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1119
Doc 3690

Intrusão doc 10

ROS nº 03.2025 - CN - CPMI - CORREIOS
Fls. Nº 1143
Doc: 3690

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, page 6-2
- Scheduling and Generating Reports, page 6-7
- Viewing Reports, page 6-8
- Saving a Generated Report as an HTML File, page 6-9
- Deleting Generated Reports, page 6-10

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1144
Doc 3690

- Editing Report Parameters, page 6-11
- Deleting Scheduled Report Templates, page 6-12

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, page 6-2
- About Audit Reports, page 6-4
- About CSA Reports, page 6-5
- About Firewall Reports, page 6-5
- About Scheduled Reports, page 6-7

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.

ECT
ROS nº 03/2005 - 28-15663-01
CPMI - CORREIOS
Fls. Nº 1145
Doc: 3690

- **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.

ROS nº 03/2005 - Fls. Nº 1146
CPMI - CORREIOS
Doc: 3690

- **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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1147
3690
Doc:

- **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.

ECT 1605 CPL - AC
ROS nº 0605-CN - CPMI - CORREIOS
Fls. Nº 1148
3690
Doc:

- **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.

CPMI - CORREIOS
1149
Fls. Nº
3690
Doc:

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1150
Doc: 3690

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.

RQS nº 03/2005 - CN - CPMI – CORREIOS
Fls. Nº 1151
Doc: 3690

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1152
Doc: 3690

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1153
3690
Doc:

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.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1154
Doc: 3690

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.

IXOS nº 08/2005 - CN - CPMI - CORREIOS
Fls. Nº 1155
3690
Doc:

Intrusão doc 11

ECT
160
L - AC

EDOS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1156
Doc 3690

Cisco Systems

White Paper

CiscoWorks **VPN/Security Management Solution** (VMS) 2.1 Deployment Guide

Introduction

The Challenge

One of the challenges of network management is the ability to have a solution that is flexible and can adapt to the changing needs of a network. While it makes sense to have applications that provide basic network management functionality regardless of function, the network environment must also be considered. In this case, it makes more sense to have a focused set of tools for management. For example, a tool that focuses on managing Quality of Service (QoS) levels is not necessarily (and most likely not) going to be very good at managing a server farm topology.

Growth and Enhancements in Network Security

If we look at the network as a strategic asset to the enterprise, network management clearly becomes an important factor in the success of the company. When we consider the evolution of business applications running across the traditional data network including e-commerce, business-to-business transactions, voice over IP (VoIP), the need to provide secure network connections grows. As a result, we have witnessed a proliferation in virtual private networks (VPNs) and an enhanced awareness of network security, setting the stage for reliable security management.

Paper Objective

The purpose of this paper is to provide guidance on how to effectively deploy CiscoWorks VPN/Security Management Solution (VMS). Covered topics include: server, installation, and operating system requirements; reference topology; metrics to monitor; and device configuration considerations. This is intended to supplement the CiscoWorks VMS Quick Start Guide and User Manual. We address such questions as: Which products are included and what are they used for? How many servers will be needed? What devices can be managed with this application? By answering these questions, we can provide some basic best practices for managing specific Cisco security technology.

What It Does Not Do

This paper does not replace User Guides (and other product documentation). It does not go into comprehensive detail about the various features or capabilities of the products.

Intended Audience

This paper is intended for audiences who are already familiar with network security, VPNs, firewalls, and intrusion detection. The audience should already have a basic understanding of these concepts and tools; our goal is to show how best to deploy CiscoWorks VMS in a production environment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1157
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

High-level Overview of CiscoWorks VMS 2.1

What Does It Do?

The CiscoWorks VMS solution is a set of integrated tools that provide a comprehensive solution for VPN and security management. CiscoWorks VMS features are positioned for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based intrusion detection systems (IDS). VMS provides key features to assist customers in the deployment, monitoring, and management of their security-specific hardware. It also provides the operational management support, software distribution, configuration archive, change-audit, and syslog management for different elements of a Cisco security infrastructure. VMS provides a scalable solution that addresses the needs of small- and large-scale VPN and security deployments.

CiscoWorks VMS 2.1 Components

The CiscoWorks VPN/Security Management Solution (CiscoWorks VMS) consists of installable software components for flexible deployment options. Table 1 lists the different CiscoWorks VMS modules and their basic usages.

Table 1 CiscoWorks VMS 2.1 Modules

VMS Module	Usage
Auto Update Server	Permits configurations to be pulled from update server
CD-One/CiscoView	Provides graphical device management
Cisco IDS Host Sensor and Console	Configures host-based IDS to protect critical servers
Cisco Secure Policy Manager	Configures Cisco PIX Firewall, Cisco IOS Software firewall, and VPN
Common services	Provides a set of common software and services for the Management Centers
Management Center for IDS Sensor	Configures network-based IDS
Management Center for PIX Firewalls	Configures PIX Firewalls
Management Center for VPN routers	Configured VPN routers
Monitoring Center for Security	Monitors network and host-based IDS events, IOS and PIX syslog
Resource Manager essentials	Provides operational management, such as software distribution, change audit, syslog analysis
VPN Monitor	Monitors IPSec-based site-to-site and remote access VPN

These components can be classified into three distinct categories: Core asset management applications, monitoring applications, and security configuration applications. This section details some of the basic features associated with each product.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1158
3690
Doc:

Core Asset Management Applications

CD-One (CiscoView)

CD-One software provides the Common Management Foundation (CMF) for CiscoWorks. This includes basic components on the management server such as the web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed from CiscoWorks VMS since it is the prerequisite for other applications. In addition to the CMF, CD-One provides the web-based CiscoView application. CiscoView provides graphical browser-based access to real-time devices status and simple network management protocol (SNMP) configuration capabilities.

CiscoWorks Resource Manager Essentials

CiscoWorks Resource Manager Essentials (RME) provides the basic network management tools for day-to-day network management, including inventory, configuration, change audit, and syslog. RME also provides additional VPN management capabilities. Network administrators can now produce device configuration, software image, and syslog reports specific for VPN environments.

Security Monitoring Applications

CiscoWorks VPN Monitor

CiscoWorks VPN Monitor allows users to monitor the status of their VPN devices and tunnels. This application collects, stores, and reports statistics for VPN-capable devices, including Cisco VPN routers, and the Cisco VPN 3000 Series Concentrator. The VPN Monitor supports the two major classes of VPNs (site-to-site and remote access) as well as multiple tunneling protocols, including Layer 2 Tunneling Protocol, Point-to-Point Tunneling Protocol (PPTP), and IP security (IPsec).

CiscoWorks Monitoring Center for Security

The CiscoWorks Monitoring Center for Security, or Security Monitor, monitors IDS events from various Cisco devices. These include network IDS sensor appliances, Cisco Catalyst® 6000 IDS modules, Cisco IOS® Software IDS syslog messages, Cisco PIX® Firewall syslog messages, and Cisco host IDS events.

Security Configuration Applications

CiscoWorks Common Services Software

CiscoWorks Common Services Software includes basic components of the management server such as the Web server, common database, polling engine, and so forth. In many deployments, this is the first CD to be installed because it is the prerequisite for the Management Center tools in the CiscoWorks VMS bundle.

CiscoWorks Management Center for VPN Routers

CiscoWorks Management Center for VPN Routers (Router MC) is a VPN configuration and deployment tool for Cisco VPN routers with Cisco IOS Software. Router MC is a Web-based application installed on top of Common Services.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CVRJ - CORREIOS
Fls. Nº 1159
Doc: 3690

CiscoWorks Management Center for PIX Firewalls

Management Center for PIX Firewalls (PIX MC) is a complete firewall and access rule policy configuration tool for Cisco PIX Firewalls. You can configure new Firewalls and import configurations from existing firewalls. PIX MC also provides a powerful tool for controlling changes made to your network, showing configuration and status changes. PIX MC is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Auto Update Server

The CiscoWorks Auto Update Server (AUS) is used to store and upgrade device configuration files and software images. Cisco PIX Firewall devices periodically contact the AUS to request configuration and software updates. In this way, PIX Firewall devices are actively kept up to date. AUS is a Web-based application installed on top of CiscoWorks Common Services.

CiscoWorks Management Center for IDS Sensors

CiscoWorks Management Center for IDS sensors (IDS MC) is an IDS configuration and deployment tool for Cisco IDS sensor appliances and Cisco IDS Modules. IDS MC is a web-based application installed on top of Common Services.

Cisco IDS Host Sensor

Working as a complementary technology to IDS MC and Security Monitor, the Cisco Host Intrusion Detection System (HIDS) application protects critical servers and hosts by integrating with the operating system. By intercepting system calls to the kernel, Cisco HIDS software can protect the users' hosts by identifying attacks and preventing access to resources and unauthorized transactions.

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) is a policy-based application that allows network and security administrators to define and deploy perimeter security policies on mixed Cisco PIX Firewalls and Cisco IOS routers with the firewall feature set. CSPM also facilitates the deployment of site-to-site, mixed-environment VPN topologies.

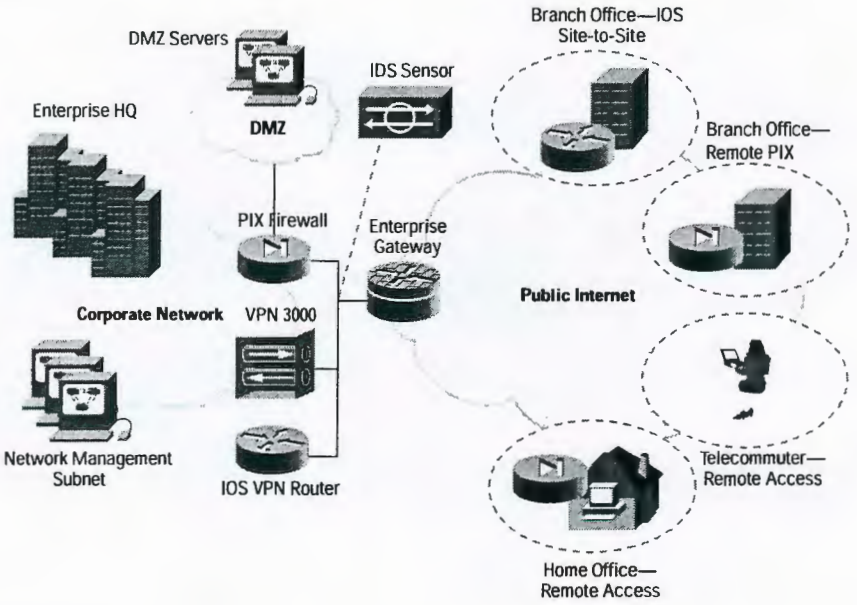
Reference Topology

In order to describe how best to deploy the CiscoWorks VMS, we will use a reference network topology that shows the different aspects of VPN and network security (Figure 1). While obviously not identical to most customer environments, it does serve to provide a holistic view of a secure network. The intent is that by providing this reference, readers will be able to select the different components that best represent their topology and hence, understand how best to deploy CiscoWorks VMS in their environment.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1160
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 1
Reference Security Topology



The infrastructure involved:

a. Enterprise Gateway: This is a Cisco IOS router with the firewall feature set. The main purpose of this device is to perform the gateway routing and the basic frontline firewall functionality.

b. Cisco PIX Firewall: The Cisco PIX Firewall provides the comprehensive firewall functionality for this enterprise network. By strategically placing these devices at network access points, the corporate network resources are protected as a result of this firewall.

c. Cisco 800, 1700, 2600, 3600, 7100 or 7200 Series routers: Cisco routers act as site-to-site VPN termination points. In a hub-and-spoke VPN topology, the high-end VPN routers act as hubs, and the small- to medium-sized routers act as spokes.

d. Cisco VPN 3000 Series Concentrator: The VPN 3000 Series Concentrator is designed to provide scalable remote access VPN termination. In this topology the concentrator terminates VPN connections with a variety of remote access environments, VPN client software, and tunneling protocols (IPSec, L2TP, PPTP).

e. Cisco VPN remote-access client software: This software allows remote access users to connect to the corporate network via VPNs.

f. Cisco IDS Network Sensor: This device sits on a network segment and passively "listens" to the traffic, inspecting it against a database of common attack signatures. It forwards IDS event information to the monitoring station.

g. Cisco host-based IDS agents: Software that sits on critical network servers that protect individual hosts from intrusion and attacks. Events are forwarded to a central monitoring console.

h. Network Management Subnet: This subnet represents a dedicated network segment for the network management servers. The components of CiscoWorks VMS will reside in this subnet to manage the different pieces of the infrastructure.

RQS II - 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1161
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

i. Demilitarized zone (DMZ) Servers: This subnet represents a dedicated network segment for publicly accessible network servers. Generally, this includes e-mail, Web, File Transfer Protocol (FTP) servers, and in our case will include the Auto Update Server.

Within our reference topologies, we will be focusing on several pieces of the infrastructure that CiscoWorks VMS manages. That is not to say that the network management applications within VMS cannot manage other pieces (such as Cisco Catalyst switches), but these are the components that should be the focal point of VMS. These components include:

Enterprise HQ

This includes the network management servers, internal firewalls, VPN termination points (both hub routers and VPN concentrators), and IDS sensors. Access to the DMZ portion of the network will be controlled by internal firewalls and also have publicly accessible servers.

Remote Access Sites

The remote access sites in our topology contain the remote Cisco PIX Firewalls, remote IOS VPN routers, and remote VPN clients. These pieces of the infrastructure are responsible for VPN termination and firewall access policy at the remote site.

Software Requirements for CiscoWorks VMS

CiscoWorks VMS is composed of a series of tools that reside on a network management server (or servers). This section covers the prerequisite software needed in order to install and run the components within VMS. Primarily, this refers to operating system (OS) support. For almost every application in the VMS bundle, the supported OS is Windows 2000 Professional or Server. This is summarized in Table 2.

Table 2 Supported OS for CiscoWorks VMS Modules

CiscoWorks VMS Module	Windows Support	Solaris Support
CD-One	X	X
Resource Manager Essentials	X	X
VPN Monitor	X	X
Common Services	X	
Management Center for PIX Firewalls	X	
Auto Update Server	X	
Management Center for VPN routers	X	
Management Center for IDS Sensor	X	
Monitoring Center for Security	X	
Cisco IDS Host Sensor and Console	X[1]	
Cisco Secure Policy Manager	X	

1. Windows NT 4.0 Server, Enterprise Server (SP4 or later), Windows 2000 Advanced Server

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT
ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1162
3690
Doc:

To run the CiscoWorks VMS components on a Windows 2000 system, the following requirements must be considered:

- Windows 2000 (Service Pack 2 or later)
- IE 5.5 SP2 or later
- ODBC Driver Manager 3.510 or later
- NTFS File System
- Do not install VMS on a server that is a:
  - Primary domain controller
  - Backup domain controller
  - Terminal server

Mitigating Threats

Now that we have the basic hardware and software requirements, we must consider how to configure the servers themselves to be ready for management. As a general security axiom, to secure hosts, pay careful attention to each of the components within the systems. Keep all systems up to date with the latest patches, fixes, and so forth. In the particular case of VMS, it is important to have the latest Windows 2000 patches and hot-fixes for security. Following is a detailed checklist of items to make sure the Windows 2000 server is ready to be used as a management server:

- Install the operating system on its own partition
- Use strong passwords
- Avoid creating network shares
- Disable unnecessary accounts
- Secure the Registry
- Apply all hot-fixes and security patches
- Disable unused and unneeded services (at a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug & Play, Protected Storage, and Security Accounts Manager. Do not install IIS.)
- Disable all network protocols except Internet Protocol (TCP/IP)
- Monitor the security of your system regularly
- Limit physical access to your server
- Do not install remote access or administration tools on the server
- Periodically run a virus scanning application on the server

Hardware Considerations for CiscoWorks VMS

Along with the software requirements, be aware of the hardware requirements for the CiscoWorks VMS bundle. Then the inherent challenge is deciding how best to deploy the different applications in the solution. Since there are eleven installable software applications, there are numerous combinations in which to deploy them.

NOS nº 03/2005 - CN - CPMI - CORREIOS
1163
Fls. Nº
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Platform and Specs

The following server system requirements are specified in the VMS bundle documentation:

- Pentium III 1GHz CPU
- 1 GB RAM
- 2 GB virtual memory
- 9 GB free hard disk space

These are minimum requirements, and consideration should be given to the difference in recommended system specifications based upon different sized networks and configurations. For example, consider three different sized configurations: small, medium, and large. The first thing to think about is scalability. In other words, how many devices equate to a small, medium, and large configuration?

Scaling

Each application within CiscoWorks VMS has a different scalability metric. Table 3 provides the theoretical maximum for each of the applications.

Table 3 Theoretical Scale Limits for CiscoWorks VMS Applications

CiscoWorks VMS Module	Scalability Metric (tested up to[1])
IDS MC	300 IDS sensors
Security Monitor	500 events/sec[2]
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices
RME	5000 devices inventory, 1000 devices availability
VPN Monitor	30 devices on dashboard (hard limit)
Cisco IDS Host Console	300 host agents

1. The theoretical scale limits define what the tools have been tested up to. The numbers are stated as a guideline to guarantee reasonable performance and user experience. Although possible, it is not recommended to exceed these metrics.
2. If the volume of security events exceeds 500/second for extended periods of time, it is recommended that users consider a monitoring product from a partner-vendor that can handle higher event volumes.

These are not software-imposed limits, but rather the scale limitations based on testing maximums. For example, if a user wants to add device number 1001 to Router MC, the software will allow it. However, from a support standpoint, we do not recommend doing this.

Also note that the specifications for the minimum recommended hardware system for CiscoWorks VMS are based on testing and performance statistics for ONE (not all) of the applications in the bundle. For example, if you are using IDS MC to manage 300 sensors (the theoretical maximum), we do NOT recommend using any other applications on that server. If you plan to heavily use more than one application within VMS, it is highly recommended to put them on separate servers.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

INPI nº 03/0095 - CN - CPMI - CORREIOS
1164
3690
Doc:

The following tables list some of the more resource-intensive applications within the bundle, and configuration is broken down into small, medium, and large configuration metrics in Tables 4-6, respectively.

Table 4 Small Configuration Metrics (reflects restricted CiscoWorks VMS license model)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	20 IDS sensors
Security Monitor	200 events/sec
PIX MC	20 PIX Firewalls
AUS	20 PIX Firewalls
Router MC	20 VPN routers
CSPM	20 devices

Table 5 Medium Configuration Metrics (This configuration represents the majority of the CiscoWorks VMS customer base):

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	100 IDS sensors
Security Monitor	300 events/sec
PIX MC	100 PIX Firewalls
AUS	100 PIX Firewalls
Router MC	100 VPN routers
CSPM	50 devices

Table 6 Large Configuration (Reflects the theoretical maximum scalability metrics.)

CiscoWorks VMS Module	Scalability Metric (up to)
IDS MC	300 IDS sensors
Security Monitor	500 events/sec
PIX MC	1000 PIX Firewalls
AUS	1000 PIX Firewalls
Router MC	1000 VPN routers
CSPM	200 devices

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1165
3690
Doc:

Server Sizing

Based on these factors, a closer examination of the recommended server sizing for each configuration is now possible. It is important to note that these specifications are minimum requirements for individual applications and are frequently exceeded in many deployments. The general rule of thumb here is, if it is necessary to choose one metric that will have the greatest affect on performance, then increase the amount of RAM. It is also important to pay attention to the scale limits of each application. If you are approaching some of those theoretical limits, it might be a good idea to increase the horsepower of your VMS server(s). For example, it is not out of the question to see a P4 2.2GHz CPU with 4 GB of RAM running VMS applications. For a general guideline, please see Table 7.

Table 7 Server Recommendations for CiscoWorks VMS Configurations

Configuration	Small	Medium	Large
CPU	PIII 1GHz	PIII 1.4GHz	P4 2.0GHz
RAM	1 GB	1.5 GB	2 GB
Virtual memory	2 GB	3 GB	4 GB
Hard disk space	9 GB	20 GB	40 GB

Server Deployment Rules of Thumb

In terms of application compatibility, there are several rules to follow:

- CD-One, RME, and VPN Monitor MUST reside on the same server.
- Router MC, IDS MC, Security Monitor, PIX MC, and AUS must be installed on top of Common Services. However, since more than one instance of Common Services can be installed, these can still be deployed across different servers.
- CD-One MUST be installed before Common Services.

Given these conditions, CiscoWorks VMS can have extremely flexible deployments. All of the components can be installed and run on a single server. On the other side of the spectrum, each of these components can be installed on its own individual server. This extreme is not practical and deployment will generally depend on a number of factors, including the following four:

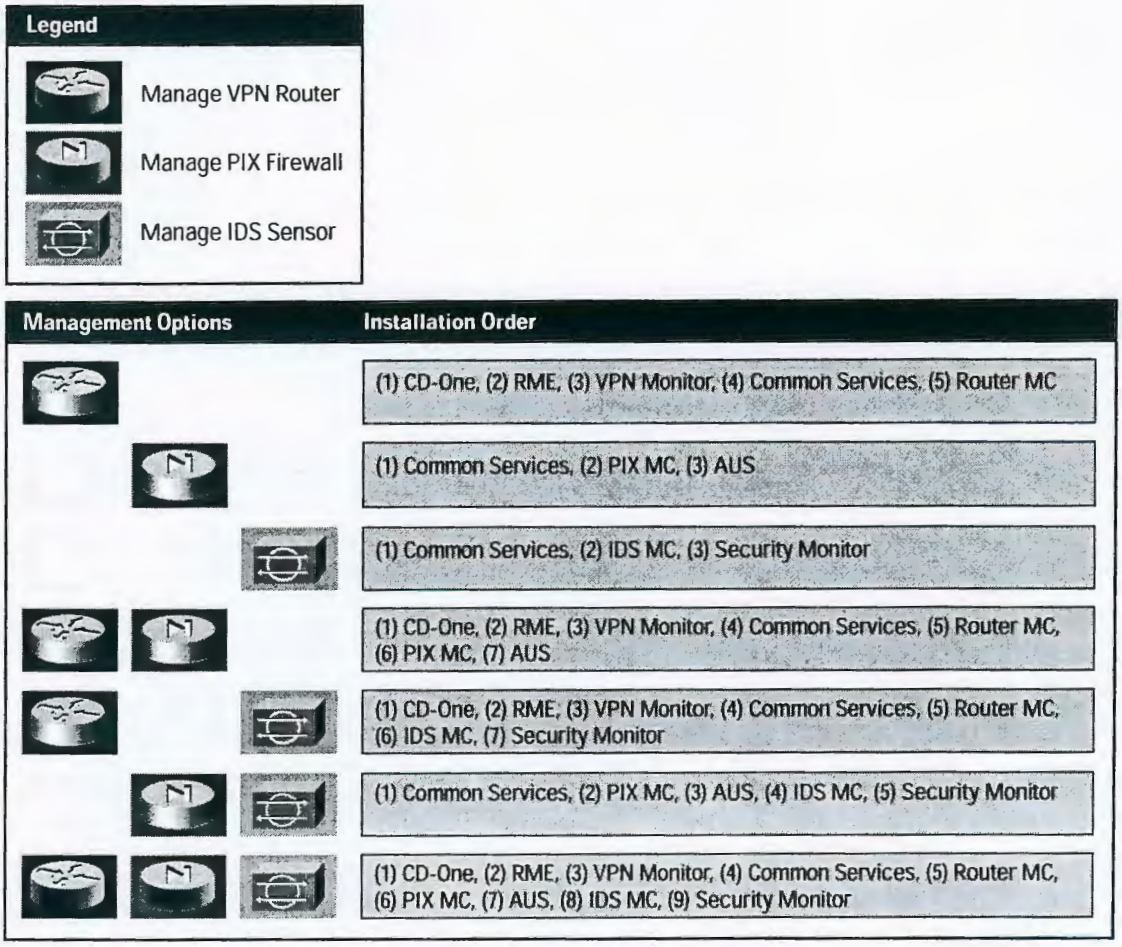
1. Which applications do you actually need?

Although VMS provides a rich, comprehensive management solution, it is possible (and perhaps even probable) that users will not need every single tool. The first question that should be asked is: Which applications do I actually need? Once this has been determined, users can choose to install only the modules that are needed. Figure 2 shows a table that provides the installation order based upon the different management options provided they are installed on a single server.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1166
Fls. Nº
3690
Doc:

Figure 2
CiscoWorks VMS Module Installation Matrix



Note: This table provides basic guidelines. Obviously, not all the combinations and tools within VMS are covered—just those with installation order dependencies.

- Installation Option 1: For VPN management, it is the monitoring component that is covered by CD-One, RME, and VPN Monitor. If monitoring is not necessary, these modules do not need to be installed.
- Installation Option 2: For PIX management, AUS is only necessary in order to take advantage of the auto-update feature for PIX configuration and software deployment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1167
3690
Doc.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2. How many devices will each application manage?

If one of the applications being used is approaching its theoretical scale limits, it is a good idea to dedicate a server to that application. For obvious reasons of resource allocation and task distribution, it is best not to have other applications using valuable CPU resources when trying to manage a large number of devices.

For example, if an instance of PIX MC is installed that is managing 800 PIX Firewalls, and the user is also trying to roll out a hub and spoke VPN deployment across 600 router spokes, it is probably a good idea to break these applications apart onto dedicated servers.

3. How many administrators will me using these applications?

In some multi-administrator environments, it makes sense to explore different deployment options for VMS. Because there are so many applications involved, and they each have a very distinct purpose, it is possible that there will be different security administrators using different applications. In this case, it is probably better to split these applications onto dedicated servers. This way, if one application is busy with a resource-intensive task such as generating configuration files, the second application will not suffer any degradation in performance.

4. What types of cost restrictions exist in terms of server procurement?

Does the organization using CiscoWorks VMS have (or have the ability to get) multiple servers? In some cases, there may only be enough budget to allocate to one server. If this is the case, then it is always better to shoot for a high-end server that exceeds the minimum system requirements. This allows room for growth, as well as improved performance.

More is Better

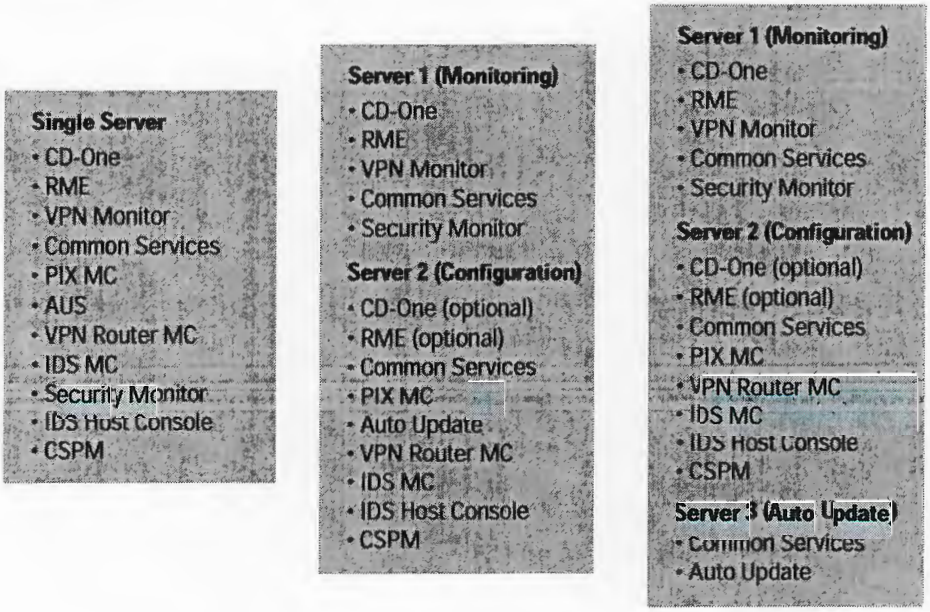
The bottom line is, if at all possible, use multiple servers and split the applications across them as they make sense. Generally, for better scalability, resource allocation, task distribution, and room for growth, more is better as long as it doesn't become cumbersome and unmanageable. Also keep in mind that if you decide to combine multiple applications onto a single server, you will need to pay special attention to the hardware requirements of each application and adjust accordingly.

The following figure and section breaks down some basic deployment options and provides some general guidelines covering most customer scenarios (Figure 3). Note that these are simply recommendations, and do not necessarily indicate that CiscoWorks VMS must be deployed in this manner.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1168
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 3
Server Deployment Options



Option 1: Single Server Deployment

For small-scale security environments with a single network security administrator, a single server deployment is recommended. This has the benefit of being low cost to the organization and guarantees ease of administration.

Option 2: 2 Servers: Configuration and Monitoring

This deployment option breaks down the VMS applications across function. One server is dedicated for monitoring and the second server is dedicated for configuration.

Server 1: Configuration

This security management server is designed to combine all of the CiscoWorks VMS applications that assist in configuration. Whether the infrastructure is VPN Router, PIX Firewall, IDS Sensor, or Host IDS Agent, this server's primary function will be configuration. The relevant applications are:

- Common Services
- PIX MC
- AUS[1]
- VPN Router MC
- IDS MC
- Cisco Host IDS Console
- Cisco Secure Policy Manager (CSPM)

1. AUS primarily provides configuration and software updates to remote PIX Firewalls. For this reason, it is frequently recommended to place the AUS within the organization's DMZ. If this is the case, we recommend using a dedicated server for AUS.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1169
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Server 2: Monitoring

The second server in this deployment option is dedicated for monitoring. VPN Monitor is used for IPsec MIB monitoring and Security Monitor is used for consolidated event viewing of Post Office IDS, Host IDS, PIX, and IOS Syslog messages. The applications for this server are:

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Option 3: 3 Servers: Security Application Function

The third deployment option centers around splitting up the CiscoWorks VMS application according to security technology (or infrastructure) managed. The first server deals with VPNs, and generally this covers IOS-based VPN routers. The second server contains the applications used to manage the PIX Firewall. Finally, the third server is dedicated to the management and monitoring of IDS—both network-based and host-based IDS.

Server 1: VPN

- CD-One
- RME
- VPN Monitor
- Common Services
- VPN Router MC

Server 2: Firewall

- Common Services
- PIX MC
- AUS
- CSPM

Server 3: IDS

- Common Services
- IDS MC
- Security Monitor
- Cisco Host IDS Console

Option 4: 4 Servers: Granular Management Control

For greater granularity and scalability benefits, further divide the deployment. The main difference with this option is the use of a dedicated server for AUS, since it is placed within a different subnet of the network. The other difference is the use of a dedicated server for the policy management tool CSPM. This makes sense because CSPM does not have any natural integration with the other products in the bundle and it is also resource intensive. As such, it is recommended to split it up and have a dedicated system for policy management across mixed environments.

ECT
CPRL - AC
ECT
ROS nº 02/2005 - CPI -
CPMI - CORREIOS
Fls. Nº 1170
DOC: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Server 1: Configuration

- Common Services
- PIX MC
- VPN Router MC
- IDS MC
- Cisco Host IDS Console

Server 2: Monitoring

- CD-One
- RME
- VPN Monitor
- Common Services
- Security Monitor

Server 3: Remote Management (placed in DMZ)

- Common Services
- AUS

Server 4: Policy

- CSPM

Again, keep in mind that these are only recommendations. There are numerous combinations and deployment options available and each case should be considered on an individual basis. There will likely be many cases where customers don't even want to use all of the possible applications within VMS.

CiscoWorks VMS Applied

Now that we have determined how to deploy the components of CiscoWorks VMS from an installation perspective, we need to take a look at how these applications should be deployed from a functional standpoint. Three basic questions will be addressed in this section:

1. What is the management function of each application?
2. What devices can I manage?
3. What types of services do I need to enable?

The first question requires a detailed look into the capabilities of each product. This information is used to figure out what aspects of security management can and should be managed by each of the components within VMS. Answering the second question will clarify confusion surrounding the variances in device support by the component applications. Finally, the last question looks at how each application touches the device(s) that it manages. By examining the communication protocols being used, we can compile a list of requirements that ensures a successful deployment of VMS. For the sake of clarity, we will examine each of the questions on a product/server basis.

Note: The components of a Cisco network infrastructure are diverse and varied; however, for this discussion surrounding security, we will focus on five classes of objects: IOS routers, PIX Firewalls, VPN concentrators, IDS sensors, and IDS host agents. This does not imply that VMS is not able to manage other elements, simply that these are the pieces we must pay special attention to for security issues.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI - CORREIOS
Fls. Nº 1171
3690

A Word About Management Subnets (Out-of-Band Management)

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices that it is trying to manage. So when making this decision, consider that, while it might be desirable to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

CD-One (CiscoView)

What is the management function?

CiscoView provides graphical Web-based device management. Users of CiscoView see a graphical representation on their computer screen and are able to monitor real-time device status, and in certain cases make configuration changes to those devices. From a CiscoWorks VMS perspective, CiscoView is positioned as a troubleshooting tool. If there is a problem within the network, and that problem has been isolated to a single device or interface, then CiscoView can be used to take a look at the statistics associated with that device and potential configure variable(s) to solve the problem.

What devices does it manage?

CiscoView provides support for the majority of the Cisco IOS routers, Cisco VPN 3000 Series Concentrators, and the Cisco PIX Firewall 501 and 506 Series.

Which services do I need to enable? (Application protocol requirements)

CiscoView relies entirely on SNMP get/set operations (UDP port 161) for its functionality. From the CiscoView server to the device, you need to enable SNMP traffic. Furthermore, the devices that you are managing must be configured to support SNMP. The Cisco IOS Software devices can support both get and set operations (for both monitoring and configuration), so both read and write community strings are configured separately to provide this level of granularity. For the VPN 3000 Concentrators and the PIX Firewalls, only SNMP read operations are supported—so while you can monitor these devices, configuration using CiscoView is not possible.

Resource Manager Essentials

What is the management function?

Describing the functions of Resource Manager Essentials (RME) would take an entire paper by itself. In general (and from a security perspective), this application provides basic network management operations and administration. Basically, this tool provides:

- Inventory management to keep track of the devices within the infrastructure
- Configuration management to manage configuration of the network devices
- Change audit control to keep track of any changes (configuration or otherwise) occurring in the network
- Software image management to facilitate the maintenance of software versions
- Syslog management to receive and analyze syslog messages sourced from the network devices

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

This list confirms that RME functionality provides benefits beyond the scope of security infrastructure management. For the purposes of this discussion, focus is on the benefits it provides to our reference environment. Of special interest is the fact that RME can generate configuration reports, software image upgrade analysis, and syslog reports specific to VPN-related infrastructure and environments.

What devices does it manage?

RME provides support for Cisco IOS routers, VPN 3000 Concentrators, and PIX Firewalls (506, 515, 520, and 525 Series). For the concentrators, RME does NOT support configuration management and only provides limited support for software image management. For the PIX Firewalls, RME provides limited support for syslog management. Refer to the diagram of our reference topology and notice this covers all aspects of our network with the exception of the IDS sensor. For this reason, RME is frequently referred to as our "core" management application.

Which services do I need to enable? (Application protocol requirements)

RME depends on several protocols to manage its devices. These include SNMP, Telnet, TFTP, and Syslog, among others. Because the subcomponents of RME are so varied, along with the different devices, we've summarized the application protocol requirements for this tool in Table 8.

Table 8 CiscoView and RME Protocol Requirements

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1173
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Based on this matrix, it is necessary to make sure the devices being managed with RME are configured to provide the proper information. SNMP read (and write where applicable) community strings need to be configured. The Telnet service, along with a login password, needs to be enabled. Finally, the devices need to be configured to point their syslog messages at the RME server.

Common Services

What is the management function?

Common Services is a server environment that provides a common set of services and management functions to a suite of client applications—the Management Centers. These services and functions include the following:

- Data storage and management
- A web infrastructure
- Session management
- User authentication/permission management
- Common environment for multiple client applications

Common Services must be installed on the server before any of the MCs, Security Monitor, or AUS can be installed. These applications integrate with Common Services and use the services and management functions provided by Common Services.

Note: To install Common Services and CD-One on the same system, CD-One MUST be installed first! Common Services can be installed on top of an existing CD-One Edition 5 installation, which allows the user to install and access applications such as RME and Router MC from a single server.

What devices does it manage?

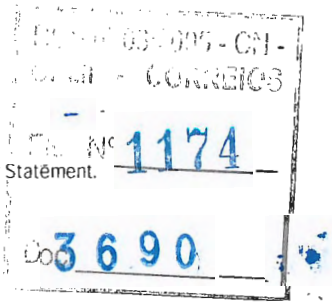
Common Services provides the server environment, and does not directly manage any particular network devices. The management is typically handled by the applications that sit on top of Common Services.

Which services do I need to enable? (Application protocol requirements)

Common Services is responsible for the web infrastructure of the VMS MC applications, so in terms of application protocols, it is important to maintain the connection from the Web client to the Web server. Typically this will be HTTP and HTTPS traffic through pre-assigned port numbers:

- TCP 1741
- TCP 1742
- TCP 1751

For a comprehensive list of TCP and UDP port numbers used by Common Services, please consult the product documentation "Installing CiscoWorks Common Services on Windows 2000."



All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Management Center for VPN Routers

What is the management function?

Management Center for VPN Routers (Router MC) provides an easy management interface to set up and maintain VPN connections between multiple supported Cisco IOS Software devices in a hub-and-spoke topology. Router MC allows network managers to quickly and easily provision all critical connectivity, security, and performance parameters for a site-to-site, large-scale VPN. Utilizing a point-and-click web-based interface and preconfigured components for VPN creation, Router MC also allows the quick configuration of smaller, simpler VPNs. In addition to configuring hub and spoke VPNs, Router MC also lets users replace leased line connections with VPN connections, or prepare VPN configurations for routers not yet on the network

What devices does it manage?

Router MC is used to manage VPNs across Cisco IOS Routers. In general, the application is hardware-platform agnostic. It only cares about the version of Cisco IOS Software and the supported feature set. The basic rule is that the routers have to support IPsec, SSH, and named access lists. Table 9 lists the Cisco IOS Software versions that have been tested with Router MC.

Table 9 Supported Cisco IOS Software Versions in Router MC

Cisco IOS Software Platform	Minimum Cisco IOS Software Version
7100, 7200 (Hub)	12.1(9)E
3640/60 (Hub)	12.2(2)T, 12.2(3)
7100, 7200 (Spoke)	12.2(2)T, 12.2(3)
2610/20/50 and 3620/40/60	12.2(2)T, 12.2(3)
1720/50	12.2(2)T, 12.2(3)
806	12.2(1)XE
803	12.2(2)XH

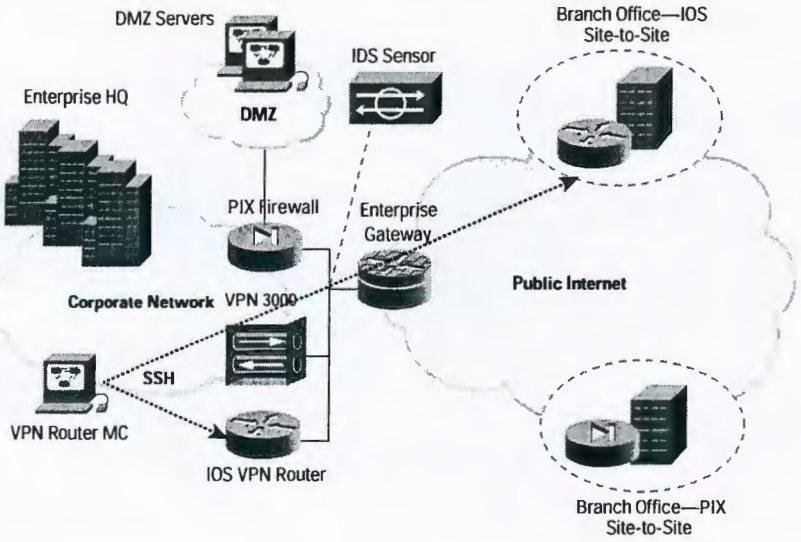
Which services need to be enabled? (Application protocol requirements)

Router MC uses SSH (TCP port 22) to configure the IOS routers. The SSH session is established when devices are initially imported into Router MC. Then when configurations are pushed out to the devices, this session is also encrypted via SSH. Figure 4 shows how Router MC is applied to our reference topology.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1175
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 4
Router MC Applied



Management Center for PIX Firewalls

What is the management function?

Management Center for PIX Firewalls (PIX MC) enables Cisco PIX Firewall infrastructure management by configuring new firewalls and importing configurations from existing firewalls. Firewall device settings, access rules, and translations rules can be configured, and these configuration changes can then be deployed to the firewalls on the network. PIX MC also provides a powerful tool for controlling changes made to the network, showing configuration and status changes.

What devices does it manage?

PIX MC is used to manage the PIX Firewall deployed throughout the network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. The PIX MC supports the command sets for PIX OS version 6.1, and supports the Auto Update and the Easy VPN command sets found in version 6.2.

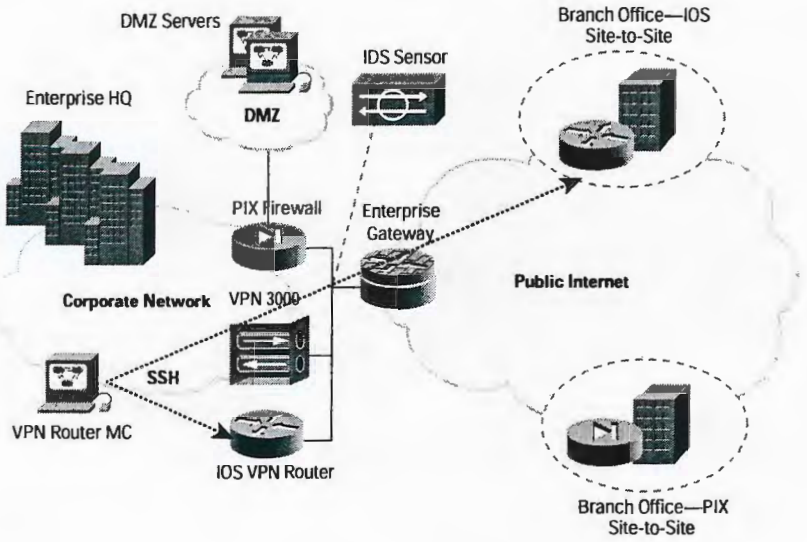
Which services must be enabled? (Application protocol requirements)

PIX MC uses an encrypted session to manage its PIX Firewall devices. The protocol that it uses is SSL (or HTTPS) and the port number assigned for this connection is TCP port 443. Therefore, it is necessary to permit TCP 443 to a PIX Firewall (from the management interface) in order for PIX MC to properly manage the device. Figure 5 shows how PIX MC is applied to our reference topology.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1176
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 5
PIX MC Applied



Auto Update Server

What is the management function?

AUS is responsible for storing configurations and software images for PIX Firewalls. Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS. Using AUS also facilitates managing devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP) or that sit behind Network Address Translation (NAT) boundaries. Typically, because of this management function, the AUS is deployed in a publicly accessible DMZ which the remote side PIX Firewalls can contact directly.

What devices does it manage?

PIX MC is used to manage the PIX Firewalls deployed throughout your network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535 Series. AUS requires that PIX Firewalls run OS version 6.2 since it requires the Auto Update feature.

Which services need to be enabled? (Application protocol requirements)

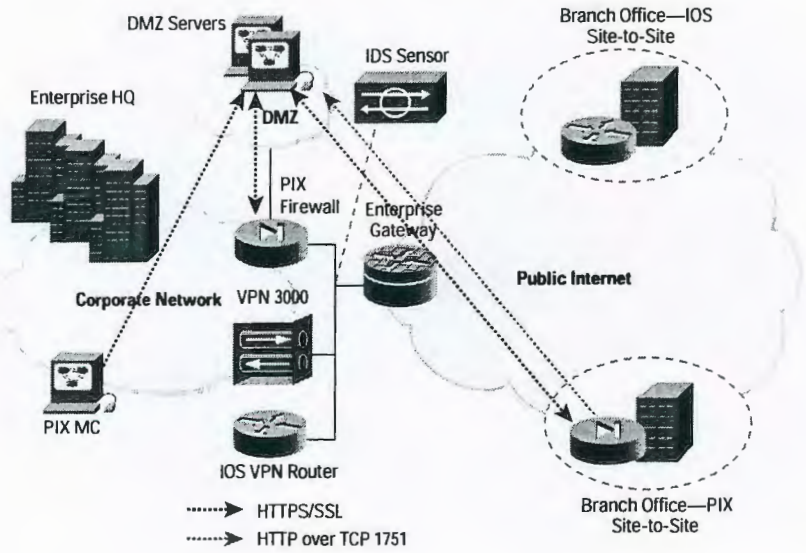
AUS talks to two different pieces in our topology diagram. The first piece it talks to is the PIX MC server. If these two applications are installed on the same system, no changes are necessary to the communication architecture. However, if they are installed on different servers, the PIX MC server will push configuration files to AUS using SSL, making it necessary to open up TCP 443 to the AUS system.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1177
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The second piece is the actual communication between the AUS and the PIX Firewall itself. In this scenario, there is two-way communication and both occur via SSL. Therefore, it is not only necessary to open up TCP 443 to the AUS from the PIX, but also vice versa. For transfer of binary images (PIX and PDM software), this will be transferred via standard HTTP over TCP 1751 (this can optionally be changed to SSL). Figure 6 illustrates how AUS is applied to our reference topology.

Figure 6
AUS Applied



Management Center for IDS

What is the management function?

Management Center for IDS (IDS MC) manages configurations for Cisco Intrusion Detection System Sensors. All aspects of sensor configuration can be managed through a series of Web-based screens, including individual sensors or a group of sensors having a common configuration. The sensor configuration data resides in a database. IDS MC can also perform signature updates by downloading the update archives from the Cisco web location and then distributing these signature updates to the appropriate sensor groups.

A separate but closely related product, Monitoring Center for Security (Security Monitor), provides event collection, viewing, and reporting capability for network devices. This is covered in the next section.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1178
Fls Nº
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

What devices does it manage?

IDS MC manages the Cisco IDS appliance sensors as well as the Cisco IDS Module for the Catalyst 6500. The IDS software required for the application depends on the platform (See Table 10).

Table 10 Required IDS Sensor Software for IDS MC

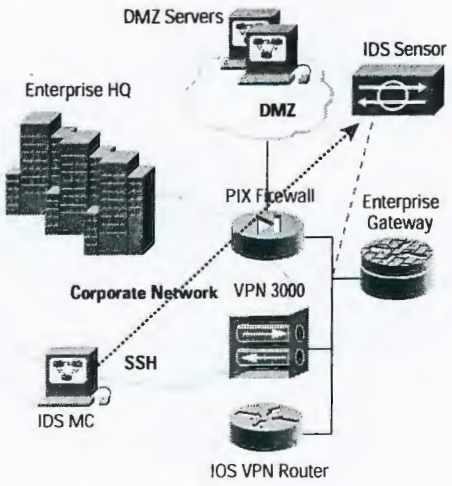
IDS Sensor Platform	Minimum Required Software
Cisco IDS Appliance Sensor	3.0.1[1]
Catalyst 6000 IDS Module	3.0.5[1]

1. IDS 4.0 software will be supported in a future release of IDS MC and Security Monitor.

Which services need to be enabled? (Application protocol requirements)

IDS MC uses two protocols to manage the IDS sensors: First, it uses Secure Shell (SSH) to secure remote login to the sensors. Second, it uses SCP to secure the transfer of the actual sensor configuration files. Session-Control Protocol (SCP) uses SSH for data transfer, so TCP 22 needs to be allowed to the sensors. Figure 7 illustrates how IDS MC is applied to our reference topology.

Figure 7
IDS MC Applied



Security Monitor

What is the management function?

Monitoring Center for Security (Security Monitor) provides a Web-based interface for event collection, viewing, and monitoring for the following devices:

- Cisco Intrusion Detection System Sensor running Post Office software
- Cisco IOS router running IDS software
- Host IDS Sensor via the Console
- PIX Firewall

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1179
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Security Monitor displays events on a customizable event viewer, and allows the user to write some basic event correlation rules to consolidate events. These rules can also be set up to kick off real time notifications.

What devices does it manage?

Security Monitor can receive security events from five sources with the following software requirements:

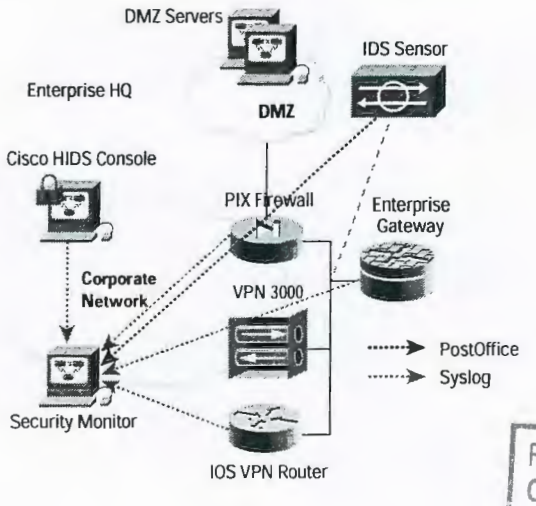
Table 11 Required Software for Security Monitor Devices

Security Event Source	Minimum Software Required
Cisco IDS Appliance Sensor	3.0.1
Catalyst 6000 IDS Module	3.0.5
IOS router	IOS with IDS features set
PIX Firewall	Any version that supports syslog
Host IDS Console	2.5 or later with integrator software

Which services do I need to enable? (Application protocol requirements)

Because of the number of data inputs, consider each of these individually in terms of application protocol requirements. For the Post Office devices (sensor appliance and IDS module), Security Monitor uses Post Office protocol to forward events. For the other data sources (Cisco IOS Software, PIX and Host IDS), the events are sent to Security Monitor via syslog. So make sure to allow Post Office (UDP 45000) and syslog (UDP 514) to the Security Monitor server. Figure 8 illustrates how Security Monitor is applied to our reference topology.

Figure 8
Security Monitor Applied



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1180
3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

VPN Monitor

What is the management function?

VPN Monitor provides monitoring statistics for the enterprise head-end VPN devices—this means the "hubs" of a hub-and-spoke VPN topology. In our reference topology, this refers to both the Cisco 7X00 Series Router and the VPN 3000 Concentrator, so proper connectivity from the VPN Monitor server to those devices is necessary. This application provides statistical VPN information in both graphical and tabular format. It can also be used as a graphical notification tool when certain VPN-related thresholds (that are user configurable) are violated. With VPN Monitor, network administrators can get an overall view of how their VPNs are doing by looking at metrics that include encrypted traffic statistics, secure handshake negotiations, packet replays, and so on.

What devices does it manage?

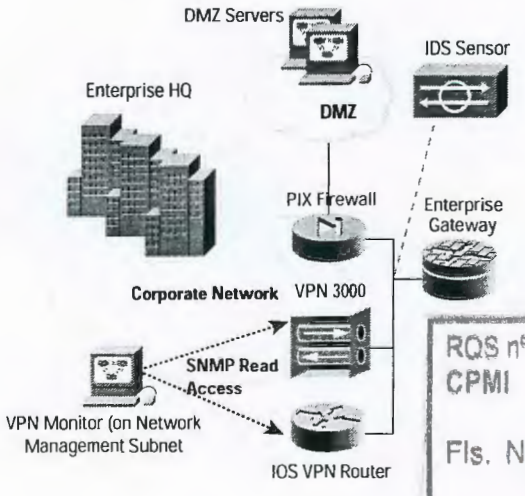
VPN Monitor supports Cisco IOS VPN routers with the necessary IPSec MIB support as well as VPN 3000 Concentrators. Currently, the application supports the Cisco1700, 2600, 3600, 7100, and 7200 Series routers. The software image version requirements are:

- 1700, 2600, or 3600 IOS Router—12.2(4)T or later
- 7100 or 7200 IOS Router—12.1(5a)E or later
- VPN Concentrator 3000 Series—2.5.2f or later

Which services do I need to enable? (Application protocol requirements)

Much like CiscoView, VPN Monitor requires SNMP (UDP port 161) to function. The VPN Monitor server periodically polls the devices to retrieve the IPSec MIB information. Since this is purely a monitoring tool, it is only necessary to consider SNMP get operations on these two classes of devices. This corresponds to configuring the SNMP read community string on the network devices that need to be managed with VPN Monitor. Figure 9 illustrates how VPN Monitor is applied to our reference topology.

Figure 9
VPN Monitor Applied



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1181
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Note: Given these requirements, it IS possible to use VPN Monitor on a remote VPN device. However, this is not entirely practical for two reasons: First, this type of monitoring does not scale as well. Second, in most cases it is sufficient to view the VPN metrics from one end of the tunnel (and not both).

Cisco IDS Host Sensor

What is the management function?

The Cisco IDS Host Sensor (Cisco HIDS) application is a product that complements the network-based IDS management provided in IDS MC and Security Monitor, and gives CiscoWorks VMS a truly comprehensive solution to manage intrusion detection. The basic premise of Cisco HIDS is to protect individual host systems from intrusion detection. The software (agent) sits on the host itself and examines system calls to the OS kernel, comparing these to a database of well-known signatures. Events are reported back to a central Cisco HIDS Console system, which consolidates the information from the agents it is managing. If a signature match is found, Cisco HIDS will prevent the operation and shoot off a real-time notification.

This protection model is proven to mitigate well-known threats such as the NIMDA and Code-Red worms without any user configuration. This means the Cisco HIDS agent software is especially important to use on important network hosts, at the user's discretion. In our reference topology, the Cisco HIDS agent code is installed on all the network management servers that comprise the VMS solution, thus protecting the important network management systems. These servers report IDS events back to the HIDS Console system, which are then forwarded to Security Monitor, provided the integrator software is installed on the HIDS Console. Users are asked to provide the IP address and syslog listening port of Security Monitor during the installation of the integrator.

What devices does it manage?

The Cisco HIDS application does not directly interact with Cisco network devices. It interacts with network hosts with the Cisco HIDS Agent code installed. At present, the following server OS versions are protected:

- Windows NT 4.x Server
- Windows NT Enterprise Server (SP 3 or later)
- Windows 2000 Server
- Windows 2000 Advanced Server
- Solaris 2.6, 2.7, and 2.8

The following Web servers are protected:

- Windows IIS Web Server
- Solaris Apache
- Solaris Netscape Enterprise
- Solaris iPlanet

Consult product documentation to verify the current available option of the Cisco HIDS Agent software.

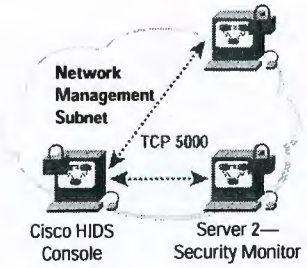
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1182
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Which services do I need to enable? (Application protocol requirements)

For Cisco HIDS to work properly, the agents must be able to communicate with the console. This is necessary so that the agents can report IDS events to the console, and just as importantly, the console can push configuration changes out to the agents. This communication is accomplished through a proprietary protocol that travels on TCP port 5000. This port number is actually a configurable option upon install, but TCP port is the default value. Figure 10 illustrates how the Cisco HIDS application is applied to our reference topology.

Figure 10
Cisco HIDS Console and Agents Applied



Cisco Secure Policy Manager

What is the management function?

Cisco Secure Policy Manager (CSPM) is an end-to-end security policy tool. Network administrators use CSPM to define and deploy security policies for their networks. This can be something as simple as what hosts or networks are allowed to access their network, or it can be something much more complex involving encryption, access methods, and other variables. The point is that, using CSPM, network administrators can implement policy management across their mixed network infrastructures.

From the perspective of our reference topology, the role of CSPM is twofold: 1. It manages traffic encryption policy by handling the VPN configuration that allows the user to configure the hub and spoke VPN tunnels between the 7X00 Series Router on the corporate network to the endpoints on the branch sites (both IOS and PIX devices). 2. It allows the user to configure security policies on the PIX Firewall(s) and also the firewall feature set on the IOS enterprise gateway, defining basic firewall policy distribution.

What devices does it manage?

As can be inferred from the previous paragraph, CSPM is able to manage the Cisco IOS routers and PIX Firewalls. The software image version requirements are:

- Cisco IOS Router—12.0(5) or later with the FW-DES feature set
- PIX Firewall—4.2.4 or later with the Data Encryption Standard (DES) feature set

Other versions can be added and managed as well, using the version management utility in CSPM.

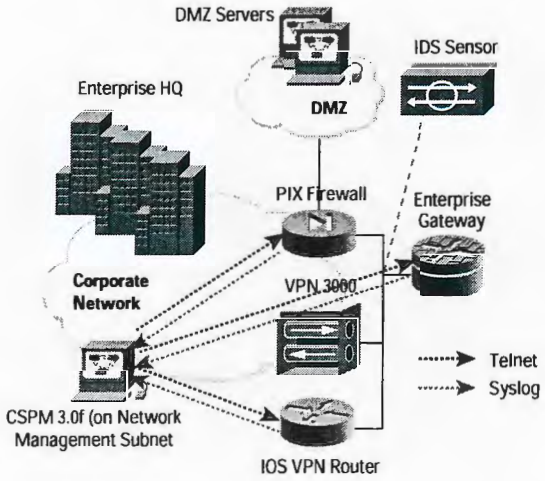
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1183
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Which services do I need to enable? (Application protocol requirements)

CSPM requires several protocols in order to function. First, when applying a security policy across the network, CSPM will use Telnet (TCP port 23) to connect to the device(s) and make configuration changes. The second protocol is syslog (UDP port 514). The CSPM has the ability to receive and consolidate syslog messages from the Cisco devices that it is managing. The application keeps an archive of these syslog messages and can use them to generate reports based upon the information they provide. Based on these requirements, the devices must then be configured to support these services. For both Cisco IOS Software and PIX, the telnet service along with a login password must be enabled. These devices also need to be configured to point their syslog messages to the CSPM server. Note that those devices managed by both RME and CSPM will now be sending their syslog messages to two different hosts. Figure 11 illustrates how CSPM is applied in our reference topology.

Figure 11
CSPM Applied



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1184
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Putting It All Together

Clearly, it is important to distinguish which components to use, determine where to deploy the various components of VMS, and identify what elements of the network infrastructure each piece manages. Table 12 summarizes the information presented in this section along with the associated management protocols that must be enabled in order for the applications to function properly.

Table 12 Summary of CiscoWorks VMS Components Applied

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

Caveats

When deploying VMS, it is important to realize the specific services required by each individual application, as outlined in the previous section. In certain instances, two different applications may require the same type of access to a particular device (for example, CiscoView and VPN Monitor both use SNMP to retrieve the management information). However, because some of the applications within VMS have a security focus, sharing access to a device can be a potentially contentious situation. This section discusses some of the things that need to be considered should you deviate from the deployment guidelines provided in this document.

Considerations with Network Address Translation

In many topologies, Network Address Translation (NAT) is used. This is an excellent feature for security and address space conservation, but it can create some problems with management tools. This section points out some of the caveats and issues that may occur if CiscoWorks VMS is deployed into a network environment with NAT.

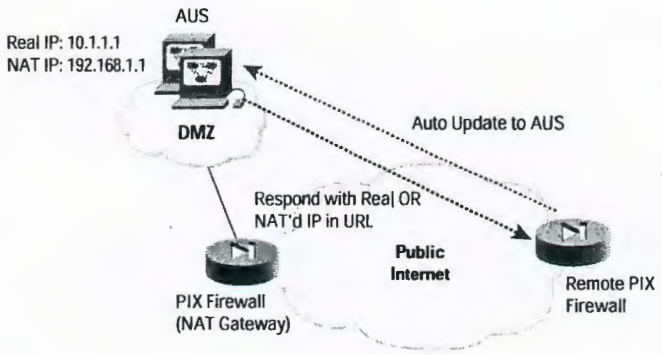
ECT 16/12/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1185
Doc 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

NAT and AUS

If the AUS application is used and the server is sitting behind a NAT gateway, pay special attention to the PIX Firewalls you are managing. Consider a remote PIX that contacts the AUS server. It will actually contact the NAT address (not the real address). When the AUS responds with the proper URL to download the updated configuration or software image, it will use the NAT address. Conversely, if the AUS is NOT behind a NAT gateway, you could also configure it to provide it's real address (Figure 12). The bottom line is that you have to decide to use the NAT address or the real address for ALL the PIX Firewalls you are managing—NAT and non-NAT addresses cannot be mixed within a single installation of AUS.

Figure 12
NAT and AUS



When it is necessary to manage PIX Firewalls (both internal and external), we recommend installing two copies of AUS—one for the external firewalls that will use the NAT address and one for the internal firewalls that will use the real IP address.

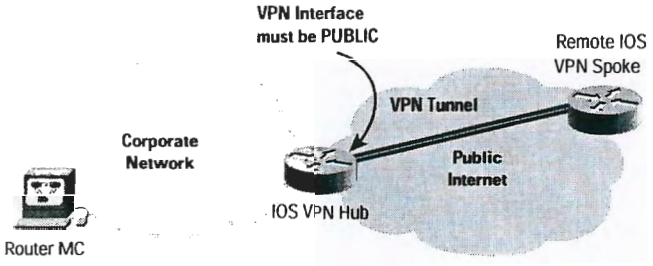
NAT and Router MC (Hub Side)

When using Router MC to set up a hub-and-spoke VPN environment, be careful about the hub router VPN interface. Because of the way the product is designed, this interface cannot be behind a NAT gateway. The VPN termination interface must be a publicly addressable IP subnet. If it was behind a NAT gateway, then from the perspective of the peer it would be necessary to assign it the NAT'd address. The Router MC application, however, only allows you to assign by interface and not IP address—so the peer statements will be incorrect. Refer to Figure 13 to see how the VPN topology must be built for compatibility with Router MC.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1186
3690
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 13
NAT and Router MC



NAT and Router MC (Spoke Side)

There is also a deployment caveat with NAT and VPN spoke devices. Router MC needs to manage the spoke devices (VPN peers) with their real IP address. The current version of Router MC does not support the situation where the spoke is behind a NAT gateway.

Managing a Device with CSPM and a MC

With the number of different applications within the VMS bundle, it is possible to have some functional overlap between tools. For example, if you want to change a PIX Firewall access rule, you can use either CSPM or PIX MC. This section describes some caveats and issues that exist when using overlapping applications.

CSPM and PIX MC

The first area of functional overlap is between CSPM and PIX MC. Both applications can be used to manage firewall device settings and access rules. So what happens when somebody tries to use both tools? Will this configuration even work?

The short answer is that this will NOT work. What will happen is when a configuration change is made using one of the applications, it will overwrite that change with the other application. This can be avoided by doing a re-import of the existing configuration before every deployment, but this is not practical. Also, you would need to make sure that you had an access rule set up to allow SSL traffic to the PIX. The recommendation here is to either use CSPM or PIX MC to manage a device, but not both.

CSPM and Router MC

The second area of functional overlap involves CSPM and Router MC. Both applications can be used to configure site-to-site VPNs on IOS VPN routers. CSPM can also be used to configure the firewall features set on those routers. Here, the consideration when each application would be used and how the two can work together.

As with PIX MC, avoid managing a single router's VPN settings with multiple applications. Even though Router MC does not push out a whole configuration file to the device (it sends out individual commands), it is possible that something will get overwritten in the original configuration. Looking at the reverse, it is definitely a problem if CSPM tries to configure a router that has already been configured with Router MC. The device will need to be re-imported into the CSPM database every time, just to make sure your configuration is current. This is also not a very practical solution. Either use CSPM or Router MC to manage a device, but not both.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Fls. Nº 1187
3690
Doc:

When To Use What

Based on some of the overlap in product functionality, it can be confusing to decide which product should be used in what situations. CSPM is currently the only product that can help manage a mixed environment, so you need to use CSPM to set up a VPN tunnel between a PIX device and an IOS device. Otherwise, since they are designed for better scalability, it is ALWAYS recommended to use the MC applications instead, based on the network environment and management needs.

Multiple Syslog Daemons

Several applications within the VMS bundle can receive syslog messages from multiple sources. Now, with Cisco modified OS support, all of these applications can also be installed on a single server. In this case, it is necessary to determine how to make all of these syslog daemons compatible.

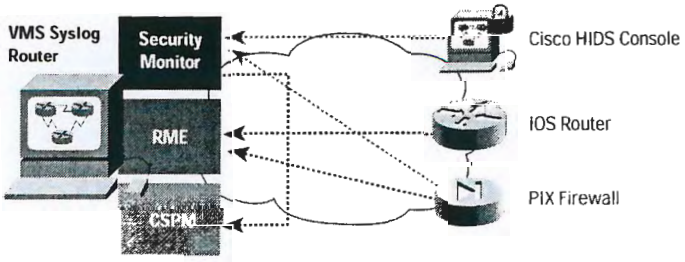
First, look at which applications can receive syslog messages, and from which devices (Table 13):

Table 13 Summary of Syslog Server Applications in VMS

CiscoWorks VMS Module	Syslog Source
RME	IOS, PIX, VPN3K
CSPM	IOS, PIX
Security Monitor	IOS, PIX, Host IDS Console

By default, all of these application listen on UDP port 514. This is not a problem if these applications are split across different servers—simply send syslog messages to multiple sources. However, what happens when all of these applications are installed on a single system AND the customer wants to try and take advantage of all three syslog daemons? (Figure 14.)

Figure 14
Syslog Consolidation in VMS



There are two ways that Security Monitor can alleviate this problem. The first is to configure what port number it should listen for syslog messages. By default it is UDP 514, but it can be changed. Also, Security Monitor can be set up to forward the syslog messages to another port on that same system. This is important because CSPM can change the port numbers they listen to for syslog messages. The other important factor is that PIX Firewalls can send syslog messages to the same host, but different port numbers. In this situation, here is the solution to maximize the syslog functionality:

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1188
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- From IOS, send syslog to RME at UDP 514
- From PIX, send syslog to RME at UDP 514
- From PIX, send syslog to Security Monitor at port x
- From Cisco HIDS Console, send syslog to Security Monitor at port x
- From Security Monitor, forward syslog to CSPM at port y

The only caveat here is that CSPM will not be able to receive IOS syslog messages.

Ideally, at least two servers would be used in this scenario to take advantage of all three tools. The first box would run Security Monitor and CSPM, and the second system would run RME. This way, no syslog functionality within VMS is lost.

Running the Cisco HIDS Software with other Applications

A major component of the CiscoWorks VMS bundle is the ability to manage IDS on a host level—or rather, to provide intrusion protection to critical servers. The management servers for VMS should definitely be considered critical and as such, we also recommend installing the Cisco HIDS agent software on these systems.

When installing another CiscoWorks VMS module on a server with Cisco HIDS, make sure the agent is in "Full Warning" mode during the install process. Running in "Full Protect" mode, it is possible that the normal operations of the software may trigger a HIDS event and, as such, may actually be prevented. In this case, a false positive would have an adverse effect on your management system by not allowing it to perform a legitimate task. In most cases, you should first install the Cisco HIDS agent and run it in "Full Warning" mode. Do this for the first several weeks of regular use to develop a baseline. This allows the user to first see events—but they will NOT be prevented. Based on this activity you can then identify any false positives and create appropriate exceptions. When the exceptions are configured, then you can change the status of your management server agents to "Full Protect" to ensure that the server is properly shielded.

Even using this deployment method, note that even in "Full Protect" mode out of the box, the HIDS agent software does not prevent any normal operations by any of the applications in the VMS bundle.

Compatibility Issues with IDS Event Viewer

Cisco IDS Event Viewer (IEV) is a Java-based application that lets users view and manage alarms from up to three IDS sensors. At the time of this writing, when IEV is installed on a PC, that PC can NOT be used as a client for the CiscoWorks VMS Web-based modules. While this compatibility limitation will be addressed in future releases, the current workarounds for this limitation are:

- Uninstall IEV from that client system
- Use a different PC as your client system

This will not be an issue for most users. Those using IDS MC and Security Monitor will most likely not need IEV as well.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1189
Doc: 3690

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Out-of-Band Management

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where the management stations reside on an isolated subnet separate from the network elements they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, CiscoWorks VMS requires network access to the devices it is trying to manage. So when making this decision, consider that, while it might be nice to have a completely isolated management subnet, it will do no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

Conclusions

Evolution of VPNs and Security

In the recent past, we have seen huge growth in the need for network security, specifically in two areas: perimeter network security and secured transactions over public infrastructure. This growth has made it necessary to evolve how a management scheme handles this environment, which has resulted in the introduction of the CiscoWorks VPN/Security Management Solution (VMS).

The CiscoWorks VMS provides customers with applications to assist in the management of their security-specific hardware such as the Cisco VPN 3000 Concentrator series, Cisco IOS VPN routers, Cisco PIX Firewalls, and Cisco IDS products. VMS addresses the challenges of VPN deployment, monitoring, development of perimeter security policies, and management of intrusion detection. This paper provides some basic deployment guidelines for VMS by outlining the different components of the solution, what they do, and how they can be configured to work together. After reading this document, the user should clearly understand how VMS fits into the network management scheme and the values it adds.

As with any dynamic environment, the needs and technologies around network security are constantly evolving. From a network management perspective, CiscoWorks VMS will continue to evolve to provide a comprehensive set of tools to manage the unique aspects of this environment.

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202881/ETMG 10/02

CORREIOS
Fls. Nº 1190
Doc:

Intrusão doc 12

RQS nº 03.[illegible]5 - CPMI - CORREIOS
Fls. Nº 1191
Doc: 3690

Release Notes for Management Center for Cisco Security Agents 4.0

These release notes are for use with Management Center for Cisco Security Agents (CSA MC) 4.0. The following information is provided:

- File Integrity Check Instructions, page 2
- New Features, page 3
- Product Documentation, page 6
- Obtaining a License Key, page 8
- IDS Host Sensor Incompatibility, page 8
- System Requirements (CSA MC), page 9
- System Requirements (Agent), page 11
- Upgrade Support, page 13
- Duplicate Configuration Naming Convention, page 13
- Cisco Security Agent Policies, page 13
- CSA MC Local Agent and Policies, page 14
- RME Gatekeeper Remote Access Issue, page 15
- Cisco VPN Client Support, page 16
- Known Problems, page 16

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1192
3690
Doc: 36

- Obtaining Documentation, page 26
- Obtaining Technical Assistance, page 28
- Obtaining Additional Publications and Information, page 31

File Integrity Check Instructions

For users who have a CCO account on Cisco.com, you can perform integrity checks on the files provided on the Startup Disk. Go to http://www.cisco.com/kobayashi/sw-center/cw2000/vms-planner.shtml to securely obtain a verify_digests.exe file. Use verify_digests.exe to check the MD5 hashes of the files you received on your product CD.

Caution When you download the digest file, make sure your browser has transitioned to https mode for a secure download.

Step 1 After you download verify_digests.exe, run it to display the precomputed valid MD5 hashes for the Startup Disk files.

Step 2 The verify_digests.exe program then prompts you for the directory of the files. Specify the Startup Disk location, press **Enter** and verify_digests.exe will validate each file.

Note You can enter the CD drive letter and check the files on the CD itself or you can copy the files to your system and check them from the directory they were copied to.

The following output is displayed:

- The output displays "OK" if the hashes match and the files are valid.
- If the hashes do not match, "Failure" is displayed. Contact Cisco if this occurs.
- If the digest program cannot locate a file, "File not found" is displayed. Check the location of the files.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1193
Fls. Nº
3690
Doc:

New Features

This release contains the following new features:

Buffer Overflow Pattern Exclusion

Use the Wizard from the Event log message in question to exclude a particular pattern when you are seeing buffer overflow events you believe are harmless.

Bulk Transfer of Hosts

Use the Bulk Transfer feature to easily move or copy all hosts from a group you select into the group you are currently viewing. This is an efficient way to move large numbers of hosts between groups.

Cisco VPN Client Support

The Cisco Security Agent is a supported configuration for the "Are You There?" feature of the Cisco VPN Client Release 4.0. For configuration details, please see the Cisco VPN Client documentation.

CSA Profiler Integrated with CSA MC

Cisco Security Agent Profiler capability is integrated and installed with CSA MC. Cisco Security Agent Profiler software works with CSA MC and Cisco Security Agent, serving as a data analysis and policy creation tool for administrators who are deploying policies across systems and networks.

Configurable Downloaded Content Application Class

CSA MC ships with a preconfigured application class called <Processes executing downloaded content>. This class includes any downloaded executable or any process that is interpreting downloaded content. If necessary, you can edit any of

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1194
3690
Doc.

these downloaded content fields and make any necessary exclusions to change the global definition of downloaded content. You may want to do this if you are experiencing false positives due to an application being seen as downloaded content

Connection Rate Limiting Rule

Use the connection rate limit rule to control the number of network connections that can be sent or received by systems within a specified time frame. This is useful in preventing attacks aimed at bringing down system services, for example, denial of service attacks (server connection rate limiting). This is also useful in preventing the propagation of denial of service attacks (client connection rate limiting).

Data Filtering—Data Access Control Rule

Use data access control rules on web servers to detect clients making malformed web server requests where such requests could crash or hang the server. A malformed request could also be an attempt by an outside client to retrieve configuration information from the web server or to run exploited code on the server.

Dynamic Application tagging in Application Control Rule

Creating dynamic application classes from the Application control rule is a bit different than creating them from other rule types. Because this rule has two application class fields, you can choose to add the current application to the dynamic class or choose to add the new application that is invoked by the first application to the dynamic class.

ECT
CPL - AC
ROS nº 00/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1195
Doc: 3690

Expanded Wizard Functionality

Use the Event Management Wizard to change the action of a rule that triggered a specific event. Through the wizard, you can automatically generate an "exception" allow rule which takes the application class and resource information in the event and creates an allow rule to counteract the rule that caused the deny.

MSDE Service Pack 3 Update

The CSA MC now installs Microsoft SQL Server Desktop Engine with Service Pack 3. This is the latest version of MSDE. Optionally, you can install your own version of SQL Server 2000 with Service Pack 3.

Network Shield System Startup Security Checks

Through this rule, you can prevent non-essential network connections during system startup. This protects the system from network-based attacks at boot-time before the agent service has started.

Rule Precedence Manipulation

In addition to ordering rules within a policy by action type, CSA MC uses the selected logging type as a way to suborder similar rules within a policy. Logging automatically takes precedence over disabled logging if the action type is the same for multiple rules in a policy. Therefore, for rules of a given priority, for example, Allow, a Log rule will be evaluated before a No Log rule.

Security Monitor Event Integration

Security Monitor can receive events from CSA MC. Refer to your Security Monitor documentation for details.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1196
3690
Doc:

VMS Integration

CSA MC is a component of the CiscoWorks VPN/Security Management Solution (VMS). You must have CiscoWorks and VMS 2.2 installed on the system on which you are installing CSA MC.

Windows Kernel Protection

Use the Kernel protection rule to detect unauthorized access to the operating system. In effect, this rule detects and logs drivers dynamically loading after boot time. Through this rule page, you can also cause the system in question to lose network connectivity when unauthorized modules are detected. This essentially quarantines the system from the network until you investigate whether the module is harmful.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

RQS nº 03/2007 - CN - CPMI - CORREIOS
Fls. Nº 1197
3690
Doc:

Table 1 Product Documentation

Document Title	Available Formats
Release Notes for Management Center for Cisco Security Agents 4.0	• Printed document that was included with the product. • On Cisco.com: a. Log into Cisco.com. – Select **Products & Services > Network Management CiscoWorks > CiscoWorks Management Center for Cisco Security Agents > Technical Documentation > Release Notes.**
Installing Management Center for Cisco Security Agents	• PDF in the top level directory on the product CD-ROM in the Documentation folder. After installation, they are also available in the CSAMC\doc subdirectory. • On Cisco.com: a. Log into Cisco.com. – Select **Products & Services > Network Management CiscoWorks > CiscoWorks Management Center for Cisco Security Agents > Technical Documentation > Installation Guides.**
Using Management Center for Cisco Security Agents	• PDF in the top level directory on the product CD-ROM in the Documentation folder. After installation, they are also available in the CSAMC\doc subdirectory. • On Cisco.com: a. Log into Cisco.com. – Select **Products & Services > Network Management CiscoWorks > CiscoWorks Management Center for Cisco Security Agents > Technical Documentation > User Guides.**

Note You must use Adobe Acrobat Reader (version 4.0 or later) to view these PDF files. You can download a free Acrobat reader from www.adobe.com.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1198
3690
Doc:

Obtaining a License Key

Before installing CSA MC, you should obtain a license key from Cisco. To receive your license key, you must use the Product Authorization Key (PAK) label affixed to the claim certificate for CSA MC located in the separate licensing envelope.

Caution CSA MC does not run on the 90-day evaluation license that other Common Services applications use. You must register CSA MC and provide the PAK to obtain a valid CSA MC license.

To obtain a production license, register your software at one of the following web sites.

If you are a registered user of Cisco.com, use this website:

http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl.

If you are not a registered user of Cisco.com, use this website:
http://www.cisco.com/pcgi-bin/Software/FormManager/formgenerator.pl.

After registration, the software license will be sent to the email address that you provided during the registration process. Retain this document with your VMS bundle product software records.

IDS Host Sensor Incompatibility

Any system on which you are installing CSA MC or the Cisco Security Agent must not have the Cisco IDS Host Sensor Console or the Cisco IDS Host Sensor installed on it. If CSA MC or the agent installer detects any Cisco IDS Host Sensor software on the system, the installation will abort.

Because there may be incompatibilities between Cisco IDS Host Sensor software and CSA MC or agent software, you must uninstall the Cisco IDS Host Sensor and Cisco IDS Host Sensor Console software before installing CSA MC or agent software. Documentation for uninstalling Cisco IDS Host Sensor software can be found at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/host/host25/install/hidsch2.htm#1024883.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1199
3690
Doc:

System Requirements (CSA MC)

CSA MC is a component of VMS.

For information on all bundle features and their requirements, see *CiscoWorks2000 VPN/Security Management Solution Quick Start Guide*.

Table 2 shows VMS bundle server requirements for Windows 2000 systems.

Table 2Server Requirements

System Component	Requirement
Hardware	• IBM PC-compatible computer • Color monitor with video card capable of 16-bit
Processor	1 GHz or faster Pentium processor
Operating System	Windows 2000 Server or Advanced Server (Service Pack 3) **Note** Terminal services are not supported on Server or Advanced Server running CSA MC.
File System	NTFS
Memory	1 GB minimum memory
Virtual Memory	2 GB virtual memory
Hard Drive Space	9 GB minimum available disk drive space **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.

RQS nº 03/20[redacted]
CPMI - CORREIOS
Fls. Nº 1200
Doc: 3690

Additional information:

- Pager alerts require a Hayes Compatible Modem.
- For optimal viewing of the CSA MC user interface, you should set your display to a resolution of 1024 x 768 or higher.
- On a system where CSA MC has never been installed, the CSA MC setup program first installs MSDE with Service Pack 3. If the CSA MC installation detects any other database type attached to an existing installation of MSDE, the installation will abort. This database configuration is not supported.

Caution **SQL Server Desktop Engine Installation**

As part of the installation process on a system where CSA MC has not been installed, the setup program first installs MSDE. When the MSDE installation completes, it may prompt you to reboot the system. In that case, you must reboot the system before restarting the CSA MC setup program. If the MSDE installation does not prompt you to reboot the system, you may restart the setup program without rebooting the system.

If the CSA MC installation detects any other database type attached to an existing installation of MSDE, the CSA MC installation will abort. This database configuration is not supported by Cisco. (Installation process aborts if any databases other than those listed here are found: master, tempdb, model, msdb, pubs, Northwind, profiler and AnalyzerLog.)

For installations exceeding 500 agents, we recommend that you install Microsoft SQL Server 2000 instead of installing the MSDE that is provided with the product. MSDE has a 2 GB limit. SQL Server 2000 must be licensed separately and it must be installed on the system before you begin installing CSA MC.

We also recommend that you format the disk to which you are installing CSA MC as NTFS. FAT32 limits all file sizes to 4 GB.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1201
3691
Doc:

System Requirements (Agent)

To run Cisco Security Agent on your Windows XP, Windows 2000 or Windows NT 4.0 servers and desktop systems, the requirements are as follows:

Table 3Agent Requirements (Windows)

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher **Note** Uni-processor, dual processor, and quad processor systems are supported.
Operating Systems	• Windows XP (Professional English128 bit) Service Pack 0 or 1 • Windows 2000 (Professional, Server or Advanced Server) with Service Pack 0, 1, 2, or 3 • Windows NT (Workstation, Server or Enterprise Server) with Service Pack 5 or later **Note** Citrix Metaframe and Citrix XP are supported. Terminal Services are supported on Windows XP and Windows 2000 (Terminal Services are not supported on Windows NT.)
Memory	128 MB minimum—all supported Windows platforms
Hard Drive Space	15 MB or higher **Note** This includes program and data.
Network	Ethernet or Dial up **Note** Maximum of 64 IP addresses supported on a system.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1202
Doc: 3690

Note Cisco Security Agent uses approximately 20 MB of memory. This applies to agents running on all supported Microsoft and Unix platforms.

To run Cisco Security Agent on your Solaris server systems, the requirements are as follows:

Table 4Agent Requirements (UNIX)

System Component	Requirement
Processor	UltraSPARC 500 MHz or higher **Note** Uniprocessor and dual processor systems are supported.
Operating Systems	Solaris 8, 64 bit **Note** If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library which can be found on the Solaris 8 Software disk (1 of 2) in the /Solaris_8/Product directory. Install using the **pkgadd -d . SUNWlibCx** command.
Memory	256 MB minimum
Hard Drive Space	15 MB or higher **Note** This includes program and data.
Network	Ethernet **Note** Maximum of 64 IP addresses supported on a system.

78-15603-01
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1203
Doc: 3690

Caution On UNIX systems running Cisco Security Agents, if you add a new type of Ethernet interface to the system, you must reboot that system twice for the agent to detect it and apply rules to it accordingly.

Upgrade Support

Upgrading from StormWatch versions 3.0 and earlier to Cisco Security Agent V4.0 is not supported.

See *Installing Management Center for Cisco Security Agents* provided as a PDF file on the product CD for product upgrade and installation instructions.

Duplicate Configuration Naming Convention

When you upgrade CSA MC, existing configurations (for example, policies and groups) are preserved. Because CSA MC ships with preconfigured items, new items may be added to preserved ones. This occurs when the upgrade process checks the existing database. If a matching item is found, the new configuration data is not copied over the existing data; rather the existing item is left as is.

If the upgrade process finds an item with the same name as a new one, but with different configuration components (for example, variables), the existing item is renamed by appending the version number (V3.2, for example) to the name. The new version is then copied into the database with no version number so that both items can co-exist in the database. Therefore, for any partial configuration item duplications that may exist after an upgrade, the item with no version number appended to its name is always the most recent version.

Cisco Security Agent Policies

CSA MC default agent kits, groups, policies, and configuration variables provide a high level of security coverage for desktops and servers. These default agent kits, groups, policies, and configuration variables cannot anticipate all possible local security policy requirements specified by your organization's management,

RQS nº 03/2005 - CN - CPMI - CORREIOS
1204
Fls. Nº
3690
Doc:

nor can they anticipate all local combinations of application usage patterns. We recommend deploying agents using the default configurations and then monitoring for possible tuning to your environment.

CSA MC Local Agent and Policies

When you install CSA MC, an agent containing the policies necessary to protect CSA MC and other CiscoWorks daemons and operations is automatically installed. The policies that are enforced by this agent protect CSA MC, other VMS products, and general CiscoWorks operations.

If you are only running CSA MC and Security Monitor as part of your VMS bundle on the CiscoWorks system, you can secure that system with a more restrictive policy that is also shipped with CSA MC but not attached to the CiscoWorks group by default. To do this, you should create a group and attach the following policies to that new group: "CiscoWorks Restrictive VMS Module", "CiscoWorks VMS Module", and the "CiscoWorks Base Security Module". Then make the CSA MC host a member of the new group (in addition to the default group to which it already belongs). This restrictive policy puts tighter restrictions on the system because it does not have to account for other VMS bundle products that might be running on the system.

Caution If you are using the default policy to protect your VMS system (not the more restrictive policy described above) you should be aware of a specific vulnerability present in Windows 2000 SP3 that the default policy does not protect against. That vulnerability is described in Microsoft article Q326830. For interoperability reasons, it is by design that the default policy protecting the VMS system does not protect against this vulnerability. To protect your VMS system against a possible denial of service or other attack using this known vulnerability, you can either deploy the more restrictive VMS policy or install Microsoft hotfix Q326830.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. - Nº 1205
3690
Doc:

Caution If you are installing or uninstalling various VMS components, and you have a Cisco Security Agent protecting the VMS bundle, you should disable the agent service before you install or uninstall any other VMS component. (You do not have to do this when installing or uninstalling CSA MC.) To disable the agent service, from a command prompt type `net stop "Cisco Security Agent"`. (You may receive a prompt asking if you want to stop the agent service. You should click **Yes**.) To enable the service, type `net start "Cisco Security Agent"`.

If you do not disable the agent service and you attempt to alter a CiscoWorks system configuration, the agent may disallow the action or it may display multiple queries to which you must respond.

RME Gatekeeper Remote Access Issue

Remote access to the CiscoWorks RME Gatekeeper daemon is not required for correct operation of any components in the VMS bundle. Therefore, remote client access to this daemon is normally disabled through a deny rule in the "CiscoWorks VMS module" policy.

If other products that require the RME Gatekeeper daemon to be accessed remotely, such as Campus Manager or ACLM, are installed on the same system as the VMS bundle, the CSAMC "CiscoWorks VMS module" policy protecting the VMS system should be modified as follows:

Step 1 Log in to CSAMC and navigate to the "CiscoWorks VMS module" policy. The policy is accessible from Configuration > Policies in the menu bar.

Step 2 After you locate the policy, click the <#>rules link to access the policy rules list.

Step 3 Change the Allow rule "CiscoWorks RME Gatekeeper daemon, server for TCP and UDP services" from Disabled to Enabled. (Select the check box beside the rule and click **Enable** in the footer frame of CSAMC. Remember to save your changes.)

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1206
Doc: 3690

Step 4 Generate rules.

Step 5 Optionally, force polling on the agent to download the rule change.

Cisco VPN Client Support

Cisco Security Agent is a supported configuration for the "Are You There?" feature of the Cisco VPN Client, Release 4.0. For configuration details, please see Chapter 1 of the *Cisco VPN Client Administrator Guide*, in the section "Configuring VPN Client Firewall Policy—Windows Only."

Known Problems

Table 5 provides information on known issues found in this release.

Table 5 Known Issues in Cisco Security Agent 4.0

Platform	Summary	Explanation
Windows and UNIX	Permitted return UDP traffic	Return traffic for permitted UDP connections will be permitted even when there is a deny rule present for UDP traffic in that direction. This is because return UDP traffic is associated with the original allowed request.
Windows XP	Frozen agent flag	Periodically, the agent flag may stop waving or may appear frozen in a tilted position until the next event is received. This is the result of a known Microsoft Windows XP issue. Refer to Microsoft Article Q323328. (This issue is purely cosmetic and the agent is continuing to function normally.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1207
3690
Doc:

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
Windows	CMF Self Test Fails for ODBC Versions	The CMF self test produces an error in the odbc.pl part of the test. This occurs because the test does not have knowledge of the MDSE SP3 ODBC drivers installed by CSA MC. MSDE SP3 drivers are dated later than those expected by the CMF self test.
Windows	ActiveX Reports and CSA MC name resolution	CSA MC ActiveX report types use the CSA MC server system name to access the ActiveX control. Therefore, ActiveX reports will not work if name resolution on the CSA MC server does not work.
Windows	SYN flood protection and potential firewall conflict	You should only apply SYN flood protection to servers that are external to your network and not protected by a firewall. Firewalls generally provide this protection. Additionally, if you apply SYN flood protection to a system that is behind a firewall, some firewalls may interfere with the CSA SYN flood connectivity algorithm. If the firewall interferes with the CSA MC algorithm, the agent will not permit the incoming connection to be established. In this case, we recommend that you disable this rule on the agent and ensure that it is enabled on your firewall.
Windows	Automatic agent software updates for dial-up users	You should not schedule Automatic software updates for dial-up users. Because dial-up users have connections of varying speeds and due to download bandwidth needs, automatic software updates may fail or time out. Better to schedule non-automatic updates and allow dial-up users to download when they are either in the office or when they can dedicate bandwidth to the download.

ECT
CPL
ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1208
Doc: 3690

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
Windows	Automatic Windows platform update triggers query rule	Windows XP and Windows 2000 provide a mechanism for automatic and user transparent software updates. These updates are prevented from installing by an agent Query User rule. The rule asks the user if software is being installed. Because the automatic update install occurs transparently, the user will likely believe that they are not installing software and will answer No. In this case, the automatic update will fail. This is not necessarily an undesired behavior and this agent rule is in place for specific security reason.
Windows	Upgrading operating systems with agent present	When upgrading operating systems, uninstall the agent first. When the new operating system is in place, you can install a new agent kit. When applying a service pack, you can disable the agent, apply the service pack, and enable the agent.
Windows	Do not support HPNA home phoneline network adapter	Although Microsoft supports networking computers using a home phoneline network adapter (HPNA), we have not tested this configuration and therefore do not officially support it.
Windows	Deploying file sharing rules	If you are deploying rules controlling existing file share access, these rules will not apply until the machine offering the file share is rebooted. A file share, previously mapped by a user, is a persistent connection. The status of this access does not change for this persistent, pre-existing connection when a agent rule is applied. When the next reboot occurs, all rules pertaining to the file share are correctly applied.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1209
3690
Doc:

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
Windows	Connectivity issues	If you encounter problems connecting to systems running the agent, you can put those agents into Test mode. Then check for connectivity again and refer to the Event log. (Also make sure the agents do not have the Cloak mode check box selected in the Network shield rule. It is selected in shipped default policies. Systems with Cloak mode enabled do not respond to pings.)
Windows	Configuring Registry sets	If you attempt to create your own Registry sets to include in a rule, you should note that the ability to restrict Registry access is a powerful tool. Critical applications may not function as a result of a misconfigured Registry restriction. Therefore, Registry values should be as specific as possible. All rules restricting Registry access should first be run in Test Mode to ensure that no unintended restrictions have been configured.
Windows	Event level log limits	There are limitations on the number of events for each event level that the database can contain. Those default limitations are located in the sysvars.cf file found in the CSAMC\cfg directory. An event is logged when these limitations are imminent. You are advised by CSA MC to purge events at that time.
UNIX	Data filter installation	On Solaris platforms, in order to use Data access control rules (on Apache or IPlanet servers) you must install the data filter manually after you install Cisco Security Agent. Unlike Windows, the Solaris installation does not detect web server software and does not install the data filter with the agent. You must always manually install it.

CPMI - CORREIOS
Fls. Nº 1210
3690
Doc:

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
UNIX	Required platform libraries and utilities	If you have the minimal Sun Solaris 8 installation (Core group) on the system to which you are installing the agent, the Solaris machine will be missing certain libraries and utilities the agent requires. Before you install the agent, you must install the "SUNWlibCx" library, which can be found on the Solaris 8 Software disk (1 of 2) in the /Solaris_8/Product directory. Install using the **pkgadd -d . SUNWlibCx** command. If you are not sure whether you have the necessary libraries installed on your Solaris system, you can check the /usr/lib/sparcv9 directory for the following library: "libCrun.so.1". If it is not there, you must install the SUNWlibCx library before installing the agent.
UNIX	Network scans appear to reveal vulnerabilities	A network port scan of a UNIX system running an agent may indicate that certain services offered by inetd are available on the system and are therefore vulnerable to various attacks. However, network access control rules which deny or reset the connection in question are applied when the incoming connection attempts to pass any data. Because the connection was technically accepted, the service may appear to be vulnerable to a scan, when, in fact, it is not: no data will pass, and the connection is dropped. Enabling Cloak mode in the Network Shield rule stops the system from responding to requests on ports where no service is listening or for ports 0-1023, where the request is always denied even when a service is listening. (Therefore, ports 0-1023 do not appear vulnerable with Cloak mode enabled.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1211
Doc: 3690

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
UNIX	Remote file sharing issue	Remote file sharing implementations, such as NFS, may cache files on the client side and briefly operate on them without contacting the server. The agent correctly enforces access rules for the Remote Clients application class (NFS accesses) on the server; however, client-side operations might briefly appear to succeed in violation of the rules. Avoid such appearances by changing an NFS server's Remote Clients app class-related rules only when clients' access to remote file systems is minimal.
UNIX	Script interpretation issue	The agent views all scripts that use the same interpreter on UNIX systems as the same application class. For example, for Application control rules, a /bin/sh shell script is seen as a /bin/sh command.
UNIX	Use resolved links rather than symbolic links	We recommend that you write File access control rules using resolved names rather than symbolic link names.
UNIX	Systems files always accessible to root	Read access to /usr/lib/*, /usr/bin/* and usr/sbin/* is always allowed to root. Any rules you may write to block this access will be ignored for users with root access. The system requires access to these files to operate.
UNIX	Agent installation path not changeable	Changing the default installation directory path for the UNIX agent will not work. The agent must always be installed in the following directory: /opt/CSCOcsa.
UNIX	Certain applications cannot kill the agent process	The default policies restrict the ability to kill the agent process to specifically defined application classes. See the *Management Center for Security Agents User Guide* for details.
UNIX	Snooping data	Snoop sees all data sent to and from the network.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1212
3690
Doc:

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
UNIX	Network rules and IPV6 addresses	Network rules work only with IPV4 addresses. **Note** The following exception:Using @local or explicitly using the address range 0 - 255.255.255.255 will include IPV6 addresses.
UNIX	Adding a new Ethernet interface	If you add a new type of Ethernet interface to a UNIX system running an agent, you must reboot that system twice for the agent to detect it and apply current policies to it.
UNIX	Default mapping for remote superuser	The default mapping for a remote superuser application accessing a machine via NFS is to an "unknown" user (and not the local superuser). Although NFS shares can be configured to override this default setting, we strongly recommend that the default setting not be overridden. Enabling such a mapping would potentially permit a remote application to impersonate the local operating system itself and bypass agent policies.

ECT
Fls. Nº 1213
Doc: 3690

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
UNIX	Inadvertently blocking access to a device	You can inadvertently block all access to a device, such as your keyboard, with a File access control rule. If this occurs, to recover, fix or delete the rule in question and generate rules. If the agent can download the new rules, your system may or may not recover immediately depending on how gracefully the service for the device failed. If rules were downloaded and the service is still not fixed, a reboot should allow the system to recover. If the agent cannot download the new rules, boot the machine into single user mode [boot -s] and enter system maintenance mode by typing in the superuser password. Then delete the current rule set by typing: [rm/opt/CSCOcsa/cfg/agent.rul] Then exit. The system will come up with the agent downloading the new "good" rule set that you have fixed.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1214
3690
Doc:

Table 5 Known Issues in Cisco Security Agent 4.0 (continued)

Platform	Summary	Explanation
UNIX	Encountering duplicate instance error during agent upgrade	If you are upgrading the UNIX agent and you encounter the following error, "There is already an instance of the package and you cannot install due to administrator rules", you must edit the file /var/sadm/install/admin/default. Change "instance=unique" to "instance=overwrite" and proceed with the upgrade.
UNIX	Buffer overflow libraries loading order may cause conflict with Binary Compatibility Package	To protect applications, the buffer overflow libraries have been built in a way which causes them to be loaded before other libraries, including libc. Applications which depend upon BCP (Binary Compatibility Package) versions of libc may not work. Specifically, the three SunOS 4.* (not Solaris) a.out executables resident in /usr/sbin which provide multi-byte codepage support for Japanese, Chinese, Chinese-Taiwan, and Korean are known not to function. If support for SunOS multi-byte codepage applications is required, the behavior of the buffer overflow libraries can be relaxed. Additional information regarding this issue is available from the TAC.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1215
3690
Doc:

Table 6 provides information on known bugs found in this release.

Table 6 Known Bugs in Cisco Security Agent 4.0

Bug ID	Summary	Description
CSCin47432	FQDN is required to connect to CiscoWorks	On a CiscoWorks installation, when CSA MC is installed, it updates the conf file to use a fully qualified domain name. None of the MC's, including CSA MC, will launch unless the fully qualified domain name is resolvable from the client and used to connect to CiscoWorks. CSA MC does not require a FQDNs. It will work in an environment where the CSA MC hostname is resolvable via DNS or windows computing environment (WINS). **Note** The environment must be consistently DNS or WINS. Mixed DNS/WINS environments are problematic. The reason FQDNs is recommended is so that agents can reach the CSA MC from anywhere (internal or external networks).
CSCin47547	Uninstall issue when SQL server is not running	During the CSA MC uninstall, a number of SQL server queries are performed. If the SQL server is not running, then these queries cause the uninstall to fail. To prevent this uninstall issue, you should not remove or stop the SQL server before uninstalling CSA MC.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1216
Doc: 3690

Table 6 Known Bugs in Cisco Security Agent 4.0 (continued)

Bug ID	Summary	Description
CSCin47564	Install issue when SQL server is not running	During the CSA MC install, a number of SQL server queries are performed. If the SQL server is not running, then these queries cause the install to fail. To prevent this install issue, you should not stop the SQL server before installing CSA MC.
CSCin45700 also see CSCeb18384	In certain install configurations, the Event Viewer's session to the server times out	This occurs when the Security Monitor is installed on the same server with certain other CiscoWorks applications (for example, RME) that require the SSLInitializer plugin. The presence of the SSLInitializer plugin causes connections from Java applets to the server to be made outside of the context of the rest of the client's (browser's) connection space. This causes connection validation attempts to fail. When the server cannot validate the Event Viewer's connection, it will not proceed to allow that applet to update its activity flags. Thus, when the Event Viewer applet is open on the screen for longer than the timeout period (on the order of 2 hours), it cannot update its session activity flags, and it will time out.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1217
Fls. Nº
3690
Doc:

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

Fls. Nº 1218
Doc: 3690

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1219
3690
Doc:

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1220
Doc: 3690

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

CPMI - CORREIOS
Fls. Nº 1221
Doc: 3690

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

ECT
CPL
ROS nº 03/2005 - CN -
CPMI - CORREIOS
1222
Fls. Nº
3690
Doc:

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the Product Documentation section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Copyright © 2003, Cisco Systems, Inc. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1220
Fls. Nº
3690
Doc:

Intrusão doc 13

Fls. Nº 1224
3690
Doc:

IDS signatures by signature ID number

993-Missed Packet Count
994-Traffic Flow Started
995-Traffic Flow Stopped
1001-IP options-Record Packet Route
1002-IP options-Timestamp
1004-IP options-Loose Source Route
1006-IP options-Strict Source Route
1100-IP Fragment Attack
1101-Unknown IP Protocol
1102-Impossible IP Packet
1103-IP Fragments Overlap
1104-IP Localhost Source Spoof
1105-Broadcast Source Address
1106-Multicast Ip Source Address
1107-RFC 1918 Addresses Seen
1108-IP Packet with Proto 11
1200-IP Fragmentation Buffer Full
1201-IP Fragment Overlap
1202-IP Fragment Overrun - Datagram Too Long
1203-IP Fragment Overwrite - Data is Overwritten
1204-IP Fragment Missing Initial Fragment
1205-IP Fragment Too Many Datagrams
1206-IP Fragment Too Small
1207-IP Fragment Too Many Frags
1208-IP Fragment Incomplete Datagram
1220-Jolt2 Fragment Reassembly DoS attack
1300-TCP Segment Overwrite
2000-ICMP Echo Reply
2001-ICMP Host Unreachable
2002-ICMP Source Quench
2003-ICMP Redirect
2004-ICMP Echo Request
2007-ICMP Timestamp Request
2008-ICMP Timestamp Reply
2011-ICMP Address Mask Request
2012-ICMP Address Mask Reply
2100-ICMP Network Sweep w/Echo
2101-ICMP Network Sweep w/Timestamp
2102-ICMP Network Sweep w/Address Mask
2150-Fragmented ICMP Traffic
2151-Large ICMP Traffic
2152-ICMP Flood
2153-Smurf
2154-Ping of Death Attack
2155-Modem DoS
3001-TCP Port Sweep

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1225
Doc: 3690

3002-TCP SYN Port Sweep
3003-TCP Frag SYN Port Sweep
3005-TCP FIN Port Sweep
3006-TCP Frag FIN Port Sweep
3010-TCP High Port Sweep
3011-TCP FIN High Port Sweep
3012-TCP Frag FIN High Port Sweep
3015-TCP Null Port Sweep
3016-TCP Frag Null Port Sweep
3020-TCP SYN FIN Port Sweep
3021-TCP Frag SYN FIN Port Sweep
3030-TCP SYN Host Sweep
3031-TCP FRAG SYN Host Sweep
3032-TCP FIN Host Sweep
3033-TCP FRAG FIN Host Sweep
3034-TCP NULL Host Sweep
3035-TCP FRAG NULL Host Sweep
3036-TCP SYN FIN Host Sweep
3037-TCP FRAG SYN FIN Host Sweep
3038-Fragmented NULL TCP Packet
3039-Fragmented Orphaned FIN packet
3040-NULL TCP Packet
3041-SYN/FIN Packet
3042-Orphaned Fin Packet
3043-Fragmented SYN/FIN Packet
3045-Queso Sweep
3046-NMAP OS Fingerprint
3050-Half-open SYN Attack
3100-Smail Attack
3101-Sendmail Invalid Recipient
3102-Sendmail Invalid Sender
3103-Sendmail Reconnaissance
3104-Archaic Sendmail Attacks
3105-Sendmail Decode Alias
3106-Mail Spam
3107-Majordomo Execute Attack
3108-MIME Overflow Bug
3109-Long SMTP Command
3110-Suspicious Mail Attachment
3111-W32 Sircam Malicious Code
3111:1-W32 Sircam Malicious Code
3112-Lotus Domino Mail Loop DoS
3114-FetchMail Arbitrary Code Execution
3115-Sendmail Data Header Overflow
3116-Netbus
3117-KLEZ worm
3118-rwhoisd format string
3119-WS_FTP STAT overflow
3120-ANTS virus
3121-Vintra MailServer EXPN DoS
3122-SMTP EXPN root Recon
3123-NetBus Pro Traffic
3124-Sendmail prescan Memory Corruption
3150-FTP Remote Command Execution
3151-FTP SYST Command Attempt
3152-FTP CWD ~root
3153-FTP Improper Address Specified
3154-FTP Improper Port Specified
3155-FTP RETR Pipe Filename Command Execution
3156-FTP STOR Pipe Filename Command Execution
3157-FTP PASV Port Spoof

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1226
Doc: 3690

3158-FTP SITE EXEC Format String
3159-FTP PASS Suspicious Length
3160-Cesar FTP Buffer Overflow
3161-FTP realpath Buffer Overflow
3162-glFtpD LIST DoS
3163-wu-ftpd heap corruption vulnerability
3164- Instant Server Mini Portal Directory Traversal
3165-FTP SITE EXEC
3166- FTP USER Suspicious Length
3167-Format String in FTP username
3168-FTP SITE EXEC Directory Traversal
3169-FTP SITE EXEC tar
3170-WS_FTP SITE CPWD Buffer Overflow
3171-Ftp Priviledged Login
3172-Ftp Cwd Overflow
3173-Long FTP Command
3174-SuperStack 3 NBX FTP DOS
3175-ProFTPD STAT DoS
3176-Cisco ONS FTP DoS
3200-WWW Phf Attack
3201-Unix Password File Access Attempt
3202-WWW .url File Requested
3203-WWW .lnk File Requested
3204-WWW .bat File Requested
3205-HTML File Has .url Link
3206-HTML File Has .lnk Link
3207-HTML File Has .bat Link
3208-WWW campas Attack
3209-WWW Glimpse Server Attack
3210-WWW IIS View Source Attack
3211-WWW IIS Hex View Source Attack
3212-WWW NPH-TEST-CGI Attack
3213-WWW TEST-CGI Attack
3214-IIS DOT DOT VIEW Attack
3215-IIS DOT DOT EXECUTE Attack
3216-WWW Directory Traversal ../..
3217-WWW php View File Attack
3218-WWW SGI Wrap Attack
3219-WWW PHP Buffer Overflow
3220-IIS Long URL Crash Bug
3221-WWW cgi-viewsource Attack
3222-WWW PHP Log Scripts Read Attack
3223-WWW IRIX cgi-handler Attack
3224-HTTP WebGais
3225-WWW websendmail File Access
3226-WWW Webdist Bug
3227-WWW Htmlscript Bug
3228-WWW Performer Bug
3229-Website Win-C-Sample Buffer Overflow
3230-Website Uploader
3231-Novell convert
3232-WWW finger attempt
3233-WWW count-cgi Overflow
3250-TCP Hijack
3251-TCP Hijacking Simplex Mode
3300-NetBIOS OOB Data
3303-Windows Guest Login
3305-Windows Password File Access
3306-Windows Registry Access
3307-Windows Redbutton Attack
3308-Windows LSARPC Access

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1227
3690
Doc:

3309-Windows SRVSVC Access
3310-Netbios Enum Share DoS
3311-SMB: remote SAM service access attempt
3312-SMB .eml email file remote access
3313-SMB suspicous password usage
3314-Windows Locator Service Overflow
3320-SMB: ADMIN$ hidden share access attempt
3321-SMB: User Enumeration
3322-SMB: Windows Share Enumeration
3323-SMB: RFPoison Attack
3324-SMB NIMDA infected file transfer
3325-Samba call_trans2open Overflow
3326-Windows Startup Folder Remote Access
3400-Sunkill
3401-Telnet-IFS Match
3402-BSD Telnet Daemon Buffer Overflow
3403-Telnet Excessive Environment Options
3404-SysV /bin/login Overflow
3405- Avirt Gateway proxy Buffer Overflow
3406-Solaris TTYPROMPT /bin/login Overflow
3450-Finger Bomb
3451-BearShare Directory Traversal
3452-gopherd halidate overflow
3453-MS NetMeeting RDS DoS
3454-Check Point Firewall Information Leak
3455-Java Web Server Cmd Exec
3456- Solaris in.fingerd Information Leak
3457-Finger root shell
3458-AIM game invite overflow
3459-ValiCert forms.exe overflow
3460-AVTronics InetServer Buffer Overflow
3461-Finger probe
3462-Finger Redirect
3463-Finger root
3464-File access in finger
3465-Finger Activity
3500-Rlogin -froot Attack
3501-Rlogin Long TERM Variable
3502-rlogin Activity
3525-IMAP Authenticate Buffer Overflow
3526-Imap Login Buffer Overflow
3530-Cisco Secure ACS Oversized TACACS+ Attack
3540-Cisco Secure ACS CSAdmin Attack
3550-POP Buffer Overflow
3551-POP User Root
3575-INN Buffer Overflow
3576-INN Control Message Exploit
3600-IOS Telnet Buffer Overflow
3601-IOS Command History Exploit
3602-Cisco IOS Identity
3603-IOS Enable Bypass
3604-Cisco Catalyst CR DoS
3650-SSH RSAREF2 Buffer Overflow
3651-SSH CRC32 Overflow
3652-SSH Gobbles
3700-CDE dtspcd overflow
3701-Oracle 9iAS Web Cache Buffer Overflow
3702-Default sa account access
3703-Squid FTP URL Buffer Overflow
3704-IIS FTP STAT Denial of Service
3705-Tivoli Storage Manager Client Acceptor Overflow

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1228
3690
Doc:

3706-MIT PGP Public Key Server Overflow
3707-Perl fingerd Command Exec
3708-AnalogX Proxy Socks4a DNS Overflow
3709-AnalogX Proxy Web Proxy Overflow
3710-Cisco Secure ACS Directory Traversal
3711-Informer FW1 auth replay DoS
3714-Oracle TNS 'Service_Name' Overflow
3728-Long pop username
3729-Long pop password
3730-Trinoo (TCP)
3731-IMail HTTP Get Buffer Overflow
3732-MSSQL xp_cmdshell Usage
3990-BackOrifice BO2K TCP Non Stealth
3991-BackOrifice BO2K TCP Stealth 1
3992-BackOrifice BO2K TCP Stealth 2
4001-UDP Port Sweep
4002-UDP Flood
4003-Nmap UDP Port Sweep
4050-UDP Bomb
4051-Snork
4052-Chargen DoS
4053-Back Orifice
4054-RIP Trace
4055-BackOrifice BO2K UDP
4056-NTPd readvar overflow
4058-UPnP LOCATION Overflow
4060-Back Orifice Ping
4061-Chargen Echo DoS
4100-Tftp Passwd File
4101-Cisco TFTPD Directory Traversal
4150-Ascend Denial of Service
4500-Cisco IOS Embedded SNMP Community Names
4501-Cisco CVCO/4K Remote Username/Password return
4502-SNMP Password Brute Force Attempt
4503-SNMP NT Info Retrieve
4504-SNMP IOS Configuration Retrieval
4505-SNMP VACM MIB Access
4506-D-Link Wireless SNMP Plain Text Password
4507-SNMP Protocol Violation
4508-Non SNMP Traffic
4509-HP Openview SNMP Hidden Community Name
4510-Solaris SNMP Hidden Community Name
4511-Avaya SNMP Hidden Community Name
4600-IOS UDP Bomb
4601-CheckPoint Firewall RDP Bypass
4601:1-CheckPoint Firewall RDP Bypass
4601:2-CheckPoint Firewall RDP Bypass
4601:3-CheckPoint Firewall RDP Bypass
4603-DHCP Discover
4604-DHCP Request
4605-DHCP Offer
4606-Cisco TFTP Long Filename Buffer Overflow
4607-Deep Throat Response
4608-Trinoo (UDP)
4609-Orinoco SNMP Info Leak
4610-Kerberos 4 User Recon
4611-D-Link DWL-900AP+ TFTP Config Retrieve
4612-Cisco IP Phone TFTP Config Retrieve
4613-TFTP Filename Buffer Overflow
4614-DHCP request overflow
4701-MS-SQL Control Overflow

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1229
3690
Doc:

5034-WWW IIS newdsn attack
5035-HTTP cgi HylaFAX Faxsurvey
5036-WWW Windows Password File Access Attempt
5037-WWW SGI MachineInfo Attack
5038-WWW wwwsql file read Bug
5039-WWW finger attempt
5040-WWW Perl Interpreter Attack
5041-WWW anyform attack
5042-WWW CGI Valid Shell Access
5043-WWW Cold Fusion Attack
5044-WWW Webcom.se Guestbook attack
5045-WWW xterm display attack
5046-WWW dumpenv.pl recon
5047-WWW Server Side Include POST attack
5048-WWW IIS BAT EXE attack
5049-WWW IIS showcode.asp access
5050-WWW IIS .htr Overflow Attack
5051-IIS Double Byte Code Page
5052-FrontPage Extensions PWD Open Attempt
5053-FrontPage _vti_bin Directory List Attempt
5054-WWWBoard Password
5055-HTTP Basic Authentication Overflow
5056-WWW Cisco IOS %% DoS
5057-WWW Sambar Samples
5058-WWW info2www Attack
5059-WWW Alibaba Attack
5060-WWW Excite AT-generate.cgi Access
5061-WWW catalog_type.asp Access
5062-WWW classifieds.cgi Attack
5063-WWW dmblparser.exe Access
5064-WWW imagemap.cgi Attack
5065-WWW IRIX infosrch.cgi Attack
5066-WWW man.sh Access
5067-WWW plusmail Attack
5068-WWW formmail.pl Access
5069-WWW whois_raw.cgi Attack
5070-WWW msadcs.dll Access
5071-WWW msacds.dll Attack
5072-WWW bizdb1-search.cgi Attack
5073-WWW EZshopper loadpage.cgi Attack
5074-WWW EZshopper search.cgi Attack
5075-WWW IIS Virtualized UNC Bug
5076-WWW webplus bug
5077-WWW Excite AT-admin.cgi Access
5078-WWW Piranha passwd attack
5079-WWW PCCS MySQL Admin Access
5080-WWW IBM WebSphere Access
5081-WWW WinNT cmd.exe Access
5083-WWW Virtual Vision FTP Browser Access
5084-WWW Alibaba Attack 2
5085-WWW IIS Source Fragment Access
5086-WWW WEBactive Logfile Access
5087-WWW Sun Java Server Access
5088-WWW Akopia MiniVend Access
5089-WWW Big Brother Directory Access
5090-WWW FrontPage htimage.exe Access
5091-WWW Cart32 Remote Admin Access
5092-WWW CGI-World Poll It Access
5093-WWW PHP-Nuke admin.php3 Access
5095-WWW CGI Script Center Account Manager Attack
5096-WWW CGI Script Center Subscribe Me Attack

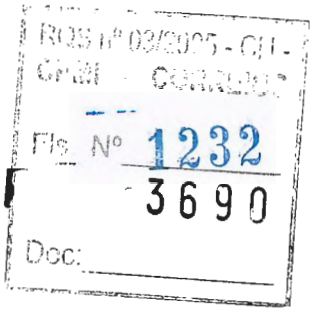
RQS nº 03/2005 - CN - CFMI - CORREIOS
Fls Nº 1230
3690
Doc:

5097-WWW FrontPage MS-DOS Device Attack
5099-WWW GWScripts News Publisher Access
5100-WWW CGI Center Auction Weaver File Access
5101-WWW CGI Center Auction Weaver Attack
5102-WWW phpPhotoAlbum explorer.php Access
5103-WWW SuSE Apache CGI Source Access
5104-WWW YaBB File Access
5105-WWW Ranson Johnson mailto.cgi Attack
5106-WWW Ranson Johnson mailform.pl Access
5107-WWW Mandrake Linux /perl Access
5108-WWW Netegrity Site Minder Access
5109-WWW Sambar Beta search.dll Access
5110-WWW SuSE Installed Packages Access
5111-WWW Solaris Answerbook 2 Access
5112-WWW Solaris Answerbook 2 Attack
5113-WWW CommuniGate Pro Access
5114-WWW IIS Unicode Attack
5115-Netscape Enterprise Server with ?wp Tags
5116-Endymion MailMan Remote Command Execution
5117-phpGroupWare Remote Command Exec
5118-eWave ServletExec 3.0C File Upload
5119-CGI Script Center News Update Admin Passwd Change
5120-Netscape Server Suite Buffer Overflow
5121-iPlanet .shtml Buffer Overflow
5122-Nokia IP440 Denial of Service
5123- WWW IIS Internet Printing Overflow
5124-IIS CGI Double Decode
5125-PerlCal Directory Traversal
5126-WWW IIS .ida Indexing Service Overflow
5127-WWW viewsrc.cgi Directory Traversal
5128-WWW nph-maillist.pl Cmd Exec
5129-IOS HTTP Unauth Command Execution
5130-Bugzilla globals.pl
5131-talkback.cgi Directory Traversal
5132-VirusScan catinfo Buffer Overflow
5133-Net.Commerce Macro Path Disclosure
5134-MacOS PWS DoS
5138-Oracle Application Server Shared Library Overflow
5140-Net.Commerce Macro Denial of Service
5141-NCM content.pl SQL Query Vulnerability
5142-DCShop File Disclosure
5143-Microsoft Media Player ASX Overflow
5146-MS-DOS Device Name DoS
5147-Arcadia Internet Store Directory Traversal Attempt
5148-Perception LiteServe Web Server CGI Script Source Code Disclosu

5149-Trend Micro Interscan Viruswall Configuration Modification
5150-InterScan VirusWall RegGo.dll Buffer Overflow
5151-WebStore Admin Bypass
5152-WebStore Command Exec
5154-WWW uDirectory Directory Traversal
5155-WWW SiteWare Editor Directory Traversal
5156-WWW Microsoft fp30reg.dll Overflow
5157-Tarantella TTAWebTop.CGI Directory Traversal Bug
5158-iPlanet Proprietary Method Overflow
5159-phpMyAdmin Cmd Exec
5160-Apache ? indexing file disclosure bug
5160:1-Apache ? indexing file disclosure bug
5161-SquirrelMail Command Exec
5162-Active Classifieds Command Exec
5163-Mambo SiteServer Administrative Password ByPass

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1231
3690
Doc:

5164-PHPBB Remote SQL Query Manipulation
5165-php-nuke article.php sql query
5166-php-nuke modules.php DoS
5167-phpMyAdmin Cmd Exec 2
5168-Snapstream PVS Directory Traversal Bug
5169-SnapStream PVS Plaintext Password Vulnerability
5170-NULL byte in URI
5171-NC-Book book.cgi Cmd Exec
5172-WinWrapper Admin Server Directory Traversal
5173-Directory Manager Cmd Exec
5174-phpmyexplorer directory traversal
5175-Hassan Shopping Cart Command Exec
5176-Exchange Address List Disclosure
5178-MS Index Server File/Path Recon
5179-PHP-Nuke File Upload
5180-sgiMerchant Directory Traversal
5181-MacOS Apache File Disclosure
5181:1-MacOS Apache File Disclosure
5182-WebDiscount's eShop Arbitrary Command Exec
5183-PHP File Inclusion Remote Exec
5184-Apache Authentication Module ByPass
5188-HTTP Tunneling
5191-Active Perl PerlIS.dll Buffer Overflow
5194-Apache Server .ht File Access
5195-AS/400 '/' attack
5196-Red Hat Stronghold Recon attack
5197-Network Query Tool command Exec
5199-W3Mail Command Exec
5200-IIS Data Stream Source Disclosure
5201-PHP-Nuke Cross Site Scripting
5202- PHP-Nuke File Copy / Delete
5203- Hosting Controller File Access and Upload
5204-AspUpload Sample Scripts
5205-Apache php.exe File Disclosure
5206-Horde IMP Session Hijack
5207-Entrust GetAccess directory traversal
5208-Network Tools shell metacharacters
5209-Agora.cgi Cross Site Scripting
5210-FAQManager.cgi directory traversal
5211-zml.cgi File Disclosure
5212-Bugzilla Admin Authorization Bypass
5213-Bugzilla Command Exec
5214-FAQManager.cgi null bytes
5215-lastlines.cgi cmd exec/traversal
5216-PHP Rocket Directory Traversal
5217-Webmin Directory Traversal
5218-Boozt Buffer Overflow
5219-Lotus Domino database DoS
5220-CSVForm Remote Command Exec
5221-Hosting Controller Directory Traversal
5223-Pi3Web Buffer Overflow
5224-SquirrelMail SquirrelSpell Command Exec
5227- AHG Search Engine Command Exec
5229- DCP Portal Root Path Disclosure
5230- Lotus Domino Authentication Bypass
5231- MRTG Directory Traversal
5232-URL with XSS
5233-PHP fileupload Buffer Overflow
5234-pforum sql-injection
5236-Xoops sql-injection
5237-HTTP CONNECT Tunnel



5238-EZNET Ezboard Buffer Overflow
5239-Sambar cgitest.exe Buffer Overflow
5240-Marcus Xenakis Shell Command Exec
5241-Avenger System Command Exec
5243-CS .cgi Script Cmd Exec
5244- PhpSmsSend Command Exec
5245- HTTP 1.1 Chunked Encoding Transfer
5246-IIS ISAPI Filter Buffer Overflow
5247-IIS ASP SSI Buffer Overflow
5248-IIS HTR ISAPI Buffer Overflow
5249-IDS Evasive Encoding
5250-IDS Evasive Double Encoding
5251-Allaire JRun // Directory Disclosure
5252-Allaire JRun Session ID Recon
5253-Axis StorPoint CD Authentication Bypass
5254-Sambar Server CGI Dos Batch File
5255-Linux Directory traceroute / nslookup Command Exec
5256-Dot Dot Slash in URI
5257-PHPNetToolpack traceroute Command Exec
5258-Script source disclosure with CodeBrws.asp
5259-Snitz Forums SQL injection
5260-Xpede sprc.asp SQL Injection
5261-BackOffice Server Web Administration Access
5262-Large number of Slashes URL
5263-ecware.exe Access
5265-RedHat cachemgr.cgi Access
5266-iCat Carbo Server File Disclosure
5268-Cisco Catalyst Remote Command Execution
5269-ColdFusion CFDOCS Directory Access
5270-EZ-Mall order.log File Access
5271-search.cgi Directory Traversal
5272-count.cgi GIF File Disclosure
5273-Bannermatic Sensitive File Access
5274-Netpad.cgi Directory Traversal/Cmd Exec
5275-Phorum Remote Cmd Exec
5276-cart.cgi Command Execution
5276:1-cart.cgi vars,env,db Recon
5276:2-cart.cgi Backdoor
5277- dfire.cgi Command Exec
5278-VP-ASP shoptest.asp access
5279-JJ CGi Cmd Exec
5280-IIS idq.dll Directory Traversal
5281-Carello add.exe Access
5282-IIS ExAir advsearch.asp Access
5282:1-IIS ExAir search.asp Access
5282:2-IIS ExAir query.asp Access
5283-info2www CGI Directory Traversal
5284- IIS webhits.dll Directory Traversal
5285-PHPEventCalendar Cmd Exec
5286-WebScripts WebBBS Cmd Exec
5287-SiteServer AdSamples SITE.CSC File Access
5288-Verity search97 Directory Traversal
5289-SQLXML ISAPI Buffer Overflow
5290-Apache Tomcat DefaultServlet File Disclosure
5291-WEB-INF Dot File Disclosure
5292-SalesCart shop.mdb File Access
5293-robots.txt File Access
5294-BearShare File Disclosure
5295-finger CGI Recon
5296-Netscape Server PageServices Directory Access
5297-order_log.dat File Access

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1233
3690
Doc:

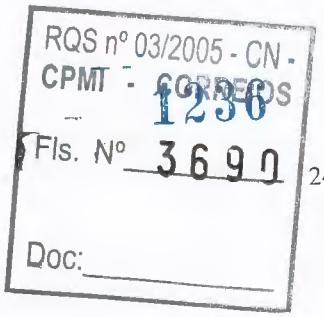
5298-shopper.conf File Access
5299-quikstore.cfg File Access
5300-reg_echo.cgi Recon
5301-/consolehelp/ CGI File Access
5302-/file/ WebLogic File Access
5303-pfdispaly.cgi Command Execution
5304-files.pl File Access
5305-.bash_history File Access
5305:1-.sh_history File Access
5305:2-.history File Access
5305:3-.zhistory File Access
5306-SoftCart storemgr.pw File Access
5308-rpc-nlog.pl Command Execution
5309- handler CGI Command Execution
5310-INDEX / directory access
5311-8.3 file name access
5312-*.jsp/*.jhtml Java Execution
5313-order.log File Access
5314- windmail.exe Command Execution
5315-changedisplay.pl WWWthreads Privilege Elevation
5316-BadBlue Admin Command Exec
5317-Tivoli Endpoint Buffer Overflow
5318-Tivoli ManagedNode Buffer Overflow
5319-SoftCart orders Directory Access
5320-ColdFusion administrator Directory Access
5321-Guest Book CGI access
5322-Long HTTP Request
5323-Cisco Router http exec command
5323-midicart.mdb File Access
5324-Cisco IOS Query (?/)
5325-Contivity cgiproc DoS
5326-Root.exe access
5327-Tilde in URI
5328- Cisco IP phone DoS
5329-Apache/mod_ssl Worm Probe
5330-Apache/mod_ssl Worm Buffer Overflow
5331-Image Javascript insertion
5332-Wordtrans-web Command Exec
5333-FUDForum File Disclosure
5334- DB4Web File Disclosure
5335-DB4WEB Proxy Scan
5336- Abyss Web Server File Disclosure
5337-Dot Dot Slash in HTTP Arguments
5338-Front Page Admin password retrival
5339-SunONE Directory Traversal
5340-Killer Protection Credential File Access
5341-HP Procurve 4000M Switch DoS
5342-Invision Board phpinfo.php Recon
5343-Apache Host Header Cross Site Scripting
5344-IIS MDAC RDS Buffer Overflow
5345-HTTPBench Information Disclosure
5346-BadBlue Information Disclosure
5347-Xoops WebChat SQL Injection
5348-Cobalt RaQ Server overflow.cgi Cmd Exec
5349-Polycom ViewStation Admin Password
5350-PHPnuke email attachment access
5351-MS IE Help Overflow
5352-H-Sphere Webshell Buffer Overflow
5353-H-Sphere Webshell 'mode' URI exec
5354-H-Sphere Webshell zipfile' URI exec
5355-DotBr exec.php3 exec

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1234
3690
Doc:

5356-DotBr system.php3 exec
5357-IMP SQL Injection
5358-Psunami.CGI Remote Command Execution
5359-Office Scan CGI Scripts Access
5360-Frontpage htimage.exe Buffer Overflow
5362-FrontPage dvwssr.dll Buffer Overflow
5363-Frontpage imagemap.exe Buffer Overflow
5364-IIS WebDAV Overflow
5365-Long WebDAV Request
5366-Shell Code in HTTP URL / Args
5367-Apache CR / LF DoS
5368-Cisco ACS Windows CSAdmin Overflow
5369-Win32 Apache Batch File CmdExec
5370-HTDig File Disclosure
5371-bdir.htr Access
5372-ASP %20 source disclosure
5373-IIS 5 Translate: f Source Disclosure
5374-IIS Executable File Command Exec
5381-VPASP SQL injection
6001-Normal SATAN Probe
6002-Heavy SATAN Probe
6050-DNS HINFO Request
6051-DNS Zone Transfer
6052-DNS Zone Transfer from High Port
6053-DNS Request for All Records
6054-DNS Version Request
6055-DNS Inverse Query Buffer Overflow
6056-DNS NXT Buffer Overflow
6057-DNS SIG Buffer Overflow
6058-DNS SRV DoS
6059-DNS TSIG Overflow
6060-DNS complain overflow
6061-DNS infoleak
6062-DNS authors request
6063-DNS Incremental zone transfer
6064-BIND Large OPT Record DoS
6100-RPC Port Registration
6101-RPC Port Unregistration
6102-RPC Dump
6103-Proxied RPC Request
6104-RPC Set Spoof
6105-RPC Unset Spoof
6110-RPC RSTATD Sweep
6111-RPC RUSERSD Sweep
6112-RPC NFS Sweep
6113-RPC MOUNTD Sweep
6114-RPC YPPASSWDD Sweep
6115-RPC SELECTION_SVC Sweep
6116-RPC REXD Sweep
6117-RPC STATUS Sweep
6118-RPC ttdb Sweep
6150-ypserv Portmap Request
6151-ypbind Portmap Request
6152-yppasswdd Portmap Request
6153-ypupdated Portmap Request
6154-ypxfrd Portmap Request
6155-mountd Portmap Request
6175-rexd Portmap Request
6180-rexd Attempt
6188-statd dot dot
6189-statd automount attack

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1235
3690
Doc:

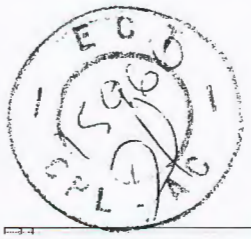
6190-statd Buffer Overflow
6191-RPC.tooltalk buffer overflow
6192-RPC mountd Buffer Overflow
6193-RPC CMSD Buffer Overflow
6194-sadmind RPC Buffer Overflow
6195-RPC amd Buffer Overflow
6196-snmpXdmid Buffer Overflow
6197-rpc yppaswdd overflow
6198-rwalld String Format
6199-cachefsd Overflow
6200-Ident Buffer Overflow
6201-Ident Newline
6210-LPRng format String Overflow
6250-FTP Authorization Failure
6251-Telnet Authorization Failure
6252-Rlogin Authorization Failure
6253-POP3 Authorization Failure
6255-SMB Authorization Failure
6275-SGI fam Attempt
6276-TooltalkDB overflow
6277-Show Mount Recon
6300-Loki ICMP Tunneling
6302-General Loki ICMP Tunneling
6350-SQL Query Abuse
6500-RingZero Trojan
6501-TFN Client Request
6502-TFN Server Reply
6503-Stacheldraht Client Request
6504-Stacheldraht Server Reply
6505-Trinoo Client Request
6506-Trinoo Server Reply
6507-TFN2K Control Traffic
6508-Mstream Control Traffic
6901-Net Flood ICMP Reply
6902-Net Flood ICMP Request
6903-Net Flood ICMP Any
6910-Net Flood UDP
6920-Net Flood TCP
7101-ARP Source Broadcast
7102-ARP Reply-to-Broadcast
7104-ARP MacAddress-Flip-Flop-Response
7105-ARP Inbalance-of-Requests
8000:2101-FTP Retrieve Password File
8000:2302-Telnet-/etc/shadow Match
8000:2303-Telnet-+ +
8000:51301-Rlogin-IFS Match
8000:51302-Rlogin-/etc/shadow Match
8000:51303-Rlogin-+ +
9000-Back Door Probe (TCP 12345)
9001-Back Door Probe (TCP 31337)
9002-Back Door Probe (TCP 1524)
9003-Back Door Probe (TCP 2773)
9004-Back Door Probe (TCP 2774)
9005-Back Door Probe (TCP 20034)
9006-Back Door Probe (TCP 27374)
9007-Back Door Probe (TCP 1234)
9008-Back Door Probe (TCP 1999)
9009-Back Door Probe (TCP 6711)
9010-Back Door Probe (TCP 6712)
9011-Back Door Probe (TCP 6713)
9012-Back Door Probe (TCP 6776)



9013-Back Door Probe (TCP 16959)
9014-Back Door Probe (TCP 27573)
9015-Back Door Probe (TCP 23432)
9016-Back Door Probe (TCP 5400)
9017-Back Door Probe (TCP 5401)
9018-Back Door Probe (TCP 2115)
9019-Back Door (UDP 2140)
9020-Back Door (UDP 47262)
9021-Back Door (UDP 2001)
9022-Back Door (UDP 2002)
9023-Back Door Probe (TCP 36794)
9024-Back Door Probe (TCP 10168)
9025-Back Door Probe (TCP 20168)
9026-Back Door Probe (TCP 1092)
9027-Back Door Probe (TCP 2018)
9028-Back Door Probe (TCP 2019)
9029-Back Door Probe (TCP 2020)
9030-Back Door Probe (TCP 2021)
9200-Back Door Response (TCP 12345)
9201-Back Door Response (TCP 31337)
9202-Back Door Response (TCP 1524)
9203-Back Door Response (TCP 2773)
9204-Back Door Response (TCP 2774)
9205-Back Door Response (TCP 20034)
9206-Back Door Response (TCP 27374)
9207-Back Door Response (TCP 1234)
9208-Back Door Response (TCP 1999)
9209-Back Door Response (TCP 6711)
9210-Back Door Response (TCP 6712)
9211-Back Door Response (TCP 6713)
9212-Back Door Response (TCP 6776)
9213-Back Door Response (TCP 16959)
9214-Back Door Response (TCP 27573)
9215-Back Door Response (TCP 23432)
9216-Back Door Response (TCP 5400)
9217-Back Door Response (TCP 5401)
9218-Back Door Response (TCP 2115)
9223-Back Door Response (TCP 36794)
9224-Back Door Response (TCP 10168)
9225-Back Door Response (TCP 20168)
9226-Back Door Response (TCP 1092)
9227-Back Door Response (TCP 2018)
9228-Back Door Response (TCP 2019)
9229-Back Door Response (TCP 2020)
9230-Back Door Response (TCP 2021)
10000:1000-IP-Spoof Interface 1
10000:1001-IP-Spoof Interface 2
11000-KaZaA v2 UDP Client Probe
11001-Gnutella Client Request
11002-Gnutella Server Reply
11003-Qtella File Request
11004-Bearshare file request
11005-KaZaA GET Request
11006-Gnucleus file request
11007-Limewire File Request
11008-Morpheus File Request
11009-Phex File Request
11010-Swapper File Request
11011-XoloX File Request
11012-GTK-Gnutella File Request
11013-Mutella File Request

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1237
Doc: 3699

11014-Hotline Client Login
11015-Hotline File Transfer
11016-Hotline Tracker Login
11200-Yahoo Messenger Activity
11201-MSN Messenger Activity
11202-AOL / ICQ Activity
11203- IRC Channel Join



BUSINESS STRATEGIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | PRODUCTS & SERVICES | TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESELLERS | ABOUT CISCO
Home | Logged In | Profile | Contacts & Feedback | Site Help
© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1238
Doc: 3690

Administrator@Carmemt

Job Title: IBM InfoPrint 20 PS, Job 42

Time Queued: Thu Jul 24 04:39:32 2003
Time Printed: Thu Jul 24 04:56:02 2003

Submitted By: Administrator@Carmemt

Need help? Call your local NCO HelpDesk.

PIO DEV: ibm@brbrap2a#IbmNetPrinter (ibm4320) @ brbraprt01

RQS nº 03/2005 - CN -
CPMI - - CORREIOS
Fls. Nº 1239
Doc: 3690

IDS signatures by signature ID number

993-Missed Packet Count
994-Traffic Flow Started
995-Traffic Flow Stopped
1001-IP options-Record Packet Route
1002-IP options-Timestamp
1004-IP options-Loose Source Route
1006-IP options-Strict Source Route
1100-IP Fragment Attack
1101-Unknown IP Protocol
1102-Impossible IP Packet
1103-IP Fragments Overlap
1104-IP Localhost Source Spoof
1105-Broadcast Source Address
1106-Multicast Ip Source Address
1107-RFC 1918 Addresses Seen
1108-IP Packet with Proto 11
1200-IP Fragmentation Buffer Full
1201-IP Fragment Overlap
1202-IP Fragment Overrun - Datagram Too Long
1203-IP Fragment Overwrite - Data is Overwritten
1204-IP Fragment Missing Initial Fragment
1205-IP Fragment Too Many Datagrams
1206-IP Fragment Too Small
1207-IP Fragment Too Many Frags
1208-IP Fragment Incomplete Datagram
1220-Jolt2 Fragment Reassembly DoS attack
1300-TCP Segment Overwrite
2000-ICMP Echo Reply
2001-ICMP Host Unreachable
2002-ICMP Source Quench
2003-ICMP Redirect
2004-ICMP Echo Request
2007-ICMP Timestamp Request
2008-ICMP Timestamp Reply
2011-ICMP Address Mask Request
2012-ICMP Address Mask Reply
2100-ICMP Network Sweep w/Echo
2101-ICMP Network Sweep w/Timestamp
2102-ICMP Network Sweep w/Address Mask
2150-Fragmented ICMP Traffic
2151-Large ICMP Traffic
2152-ICMP Flood
2153-Smurf
2154-Ping of Death Attack
2155-Modem DoS
3001-TCP Port Sweep

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1240
Doc: 3690

3002-TCP SYN Port Sweep
3003-TCP Frag SYN Port Sweep
3005-TCP FIN Port Sweep
3006-TCP Frag FIN Port Sweep
3010-TCP High Port Sweep
3011-TCP FIN High Port Sweep
3012-TCP Frag FIN High Port Sweep
3015-TCP Null Port Sweep
3016-TCP Frag Null Port Sweep
3020-TCP SYN FIN Port Sweep
3021-TCP Frag SYN FIN Port Sweep
3030-TCP SYN Host Sweep
3031-TCP FRAG SYN Host Sweep
3032-TCP FIN Host Sweep
3033-TCP FRAG FIN Host Sweep
3034-TCP NULL Host Sweep
3035-TCP FRAG NULL Host Sweep
3036-TCP SYN FIN Host Sweep
3037-TCP FRAG SYN FIN Host Sweep
3038-Fragmented NULL TCP Packet
3039-Fragmented Orphaned FIN packet
3040-NULL TCP Packet
3041-SYN/FIN Packet
3042-Orphaned Fin Packet
3043-Fragmented SYN/FIN Packet
3045-Queso Sweep
3046-NMAP OS Fingerprint
3050-Half-open SYN Attack
3100-Smail Attack
3101-Sendmail Invalid Recipient
3102-Sendmail Invalid Sender
3103-Sendmail Reconnaissance
3104-Archaic Sendmail Attacks
3105-Sendmail Decode Alias
3106-Mail Spam
3107-Majordomo Execute Attack
3108-MIME Overflow Bug
3109-Long SMTP Command
3110-Suspicious Mail Attachment
3111-W32 Sircam Malicious Code
3111:1-W32 Sircam Malicious Code
3112-Lotus Domino Mail Loop DoS
3114-FetchMail Arbitrary Code Execution
3115-Sendmail Data Header Overflow
3116-Netbus
3117-KLEZ worm
3118-rwhoisd format string
3119-WS_FTP STAT overflow
3120-ANTS virus
3121-Vintra MailServer EXPN DoS
3122-SMTP EXPN root Recon
3123-NetBus Pro Traffic
3124-Sendmail prescan Memory Corruption
3150-FTP Remote Command Execution
3151-FTP SYST Command Attempt
3152-FTP CWD ~root
3153-FTP Improper Address Specified
3154-FTP Improper Port Specified
3155-FTP RETR Pipe Filename Command Execution
3156-FTP STOR Pipe Filename Command Execution
3157-FTP PASV Port Spoof

3158-FTP SITE EXEC Format String
3159-FTP PASS Suspicious Length
3160-Cesar FTP Buffer Overflow
3161-FTP realpath Buffer Overflow
3162-glFtpD LIST DoS
3163-wu-ftpd heap corruption vulnerability
3164- Instant Server Mini Portal Directory Traversal
3165-FTP SITE EXEC
3166- FTP USER Suspicious Length
3167-Format String in FTP username
3168-FTP SITE EXEC Directory Traversal
3169-FTP SITE EXEC tar
3170-WS_FTP SITE CPWD Buffer Overflow
3171-Ftp Priviledged Login
3172-Ftp Cwd Overflow
3173-Long FTP Command
3174-SuperStack 3 NBX FTP DOS
3175-ProFTPD STAT DoS
3176-Cisco ONS FTP DoS
3200-WWW Phf Attack
3201-Unix Password File Access Attempt
3202-WWW .url File Requested
3203-WWW .lnk File Requested
3204-WWW .bat File Requested
3205-HTML File Has .url Link
3206-HTML File Has .lnk Link
3207-HTML File Has .bat Link
3208-WWW campas Attack
3209-WWW Glimpse Server Attack
3210-WWW IIS View Source Attack
3211-WWW IIS Hex View Source Attack
3212-WWW NPH-TEST-CGI Attack
3213-WWW TEST-CGI Attack
3214-IIS DOT DOT VIEW Attack
3215-IIS DOT DOT EXECUTE Attack
3216-WWW Directory Traversal ../..
3217-WWW php View File Attack
3218-WWW SGI Wrap Attack
3219-WWW PHP Buffer Overflow
3220-IIS Long URL Crash Bug
3221-WWW cgi-viewsource Attack
3222-WWW PHP Log Scripts Read Attack
3223-WWW IRIX cgi-handler Attack
3224-HTTP WebGais
3225-WWW websendmail File Access
3226-WWW Webdist Bug
3227-WWW Htmlscript Bug
3228-WWW Performer Bug
3229-Website Win-C-Sample Buffer Overflow
3230-Website Uploader
3231-Novell convert
3232-WWW finger attempt
3233-WWW count-cgi Overflow
3250-TCP Hijack
3251-TCP Hijacking Simplex Mode
3300-NetBIOS OOB Data
3303-Windows Guest Login
3305-Windows Password File Access
3306-Windows Registry Access
3307-Windows Redbutton Attack
3308-Windows LSARPC Access

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1242
3690
Doc:

3309-Windows SRVSVC Access
3310-Netbios Enum Share DoS
3311-SMB: remote SAM service access attempt
3312-SMB .eml email file remote access
3313-SMB suspicous password usage
3314-Windows Locator Service Overflow
3320-SMB: ADMIN$ hidden share access attempt
3321-SMB: User Enumeration
3322-SMB: Windows Share Enumeration
3323-SMB: RFPoison Attack
3324-SMB NIMDA infected file transfer
3325-Samba call_trans2open Overflow
3326-Windows Startup Folder Remote Access
3400-Sunkill
3401-Telnet-IFS Match
3402-BSD Telnet Daemon Buffer Overflow
3403-Telnet Excessive Environment Options
3404-SysV /bin/login Overflow
3405- Avirt Gateway proxy Buffer Overflow
3406-Solaris TTYPROMPT /bin/login Overflow
3450-Finger Bomb
3451-BearShare Directory Traversal
3452-gopherd halidate overflow
3453-MS NetMeeting RDS DoS
3454-Check Point Firewall Information Leak
3455-Java Web Server Cmd Exec
3456- Solaris in.fingerd Information Leak
3457-Finger root shell
3458-AIM game invite overflow
3459-ValiCert forms.exe overflow
3460-AVTronics InetServer Buffer Overflow
3461-Finger probe
3462-Finger Redirect
3463-Finger root
3464-File access in finger
3465-Finger Activity
3500-Rlogin -froot Attack
3501-Rlogin Long TERM Variable
3502-rlogin Activity
3525-IMAP Authenticate Buffer Overflow
3526-Imap Login Buffer Overflow
3530-Cisco Secure ACS Oversized TACACS+ Attack
3540-Cisco Secure ACS CSAdmin Attack
3550-POP Buffer Overflow
3551-POP User Root
3575-INN Buffer Overflow
3576-INN Control Message Exploit
3600-IOS Telnet Buffer Overflow
3601-IOS Command History Exploit
3602-Cisco IOS Identity
3603-IOS Enable Bypass
3604-Cisco Catalyst CR DoS
3650-SSH RSAREF2 Buffer Overflow
3651-SSH CRC32 Overflow
3652-SSH Gobbles
3700-CDE dtspcd overflow
3701-Oracle 9iAS Web Cache Buffer Overflow
3702-Default sa account access
3703-Squid FTP URL Buffer Overflow
3704-IIS FTP STAT Denial of Service
3705-Tivoli Storage Manager Client Acceptor Overflow

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1243
3690
Doc:

3706-MIT PGP Public Key Server Overflow
3707-Perl fingerd Command Exec
3708-AnalogX Proxy Socks4a DNS Overflow
3709-AnalogX Proxy Web Proxy Overflow
3710-Cisco Secure ACS Directory Traversal
3711-Informer FW1 auth replay DoS
3714-Oracle TNS 'Service_Name' Overflow
3728-Long pop username
3729-Long pop password
3730-Trinoo (TCP)
3731-IMail HTTP Get Buffer Overflow
3732-MSSQL xp_cmdshell Usage
3990-BackOrifice BO2K TCP Non Stealth
3991-BackOrifice BO2K TCP Stealth 1
3992-BackOrifice BO2K TCP Stealth 2
4001-UDP Port Sweep
4002-UDP Flood
4003-Nmap UDP Port Sweep
4050-UDP Bomb
4051-Snork
4052-Chargen DoS
4053-Back Orifice
4054-RIP Trace
4055-BackOrifice BO2K UDP
4056-NTPd readvar overflow
4058-UPnP LOCATION Overflow
4060-Back Orifice Ping
4061-Chargen Echo DoS
4100-Tftp Passwd File
4101-Cisco TFTPD Directory Traversal
4150-Ascend Denial of Service
4500-Cisco IOS Embedded SNMP Community Names
4501-Cisco CVCO/4K Remote Username/Password return
4502-SNMP Password Brute Force Attempt
4503-SNMP NT Info Retrieve
4504-SNMP IOS Configuration Retrieval
4505-SNMP VACM MIB Access
4506-D-Link Wireless SNMP Plain Text Password
4507-SNMP Protocol Violation
4508-Non SNMP Traffic
4509-HP Openview SNMP Hidden Community Name
4510-Solaris SNMP Hidden Community Name
4511-Avaya SNMP Hidden Community Name
4600-IOS UDP Bomb
4601-CheckPoint Firewall RDP Bypass
4601:1-CheckPoint Firewall RDP Bypass
4601:2-CheckPoint Firewall RDP Bypass
4601:3-CheckPoint Firewall RDP Bypass
4603-DHCP Discover
4604-DHCP Request
4605-DHCP Offer
4606-Cisco TFTP Long Filename Buffer Overflow
4607-Deep Throat Response
4608-Trinoo (UDP)
4609-Orinoco SNMP Info Leak
4610-Kerberos 4 User Recon
4611-D-Link DWL-900AP+ TFTP Config Retrieve
4612-Cisco IP Phone TFTP Config Retrieve
4613-TFTP Filename Buffer Overflow
4614-DHCP request overflow
4701-MS-SQL Control Overflow

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1244
Fls. Nº
3690
Doc:

5034-WWW IIS newdsn attack
5035-HTTP cgi HylaFAX Faxsurvey
5036-WWW Windows Password File Access Attempt
5037-WWW SGI MachineInfo Attack
5038-WWW wwwsql file read Bug
5039-WWW finger attempt
5040-WWW Perl Interpreter Attack
5041-WWW anyform attack
5042-WWW CGI Valid Shell Access
5043-WWW Cold Fusion Attack
5044-WWW Webcom.se Guestbook attack
5045-WWW xterm display attack
5046-WWW dumpenv.pl recon
5047-WWW Server Side Include POST attack
5048-WWW IIS BAT EXE attack
5049-WWW IIS showcode.asp access
5050-WWW IIS .htr Overflow Attack
5051-IIS Double Byte Code Page
5052-FrontPage Extensions PWD Open Attempt
5053-FrontPage _vti_bin Directory List Attempt
5054-WWWBoard Password
5055-HTTP Basic Authentication Overflow
5056-WWW Cisco IOS %% DoS
5057-WWW Sambar Samples
5058-WWW info2www Attack
5059-WWW Alibaba Attack
5060-WWW Excite AT-generate.cgi Access
5061-WWW catalog_type.asp Access
5062-WWW classifieds.cgi Attack
5063-WWW dmblparser.exe Access
5064-WWW imagemap.cgi Attack
5065-WWW IRIX infosrch.cgi Attack
5066-WWW man.sh Access
5067-WWW plusmail Attack
5068-WWW formmail.pl Access
5069-WWW whois_raw.cgi Attack
5070-WWW msadcs.dll Access
5071-WWW msacds.dll Attack
5072-WWW bizdb1-search.cgi Attack
5073-WWW EZshopper loadpage.cgi Attack
5074-WWW EZshopper search.cgi Attack
5075-WWW IIS Virtualized UNC Bug
5076-WWW webplus bug
5077-WWW Excite AT-admin.cgi Access
5078-WWW Piranha passwd attack
5079-WWW PCCS MySQL Admin Access
5080-WWW IBM WebSphere Access
5081-WWW WinNT cmd.exe Access
5083-WWW Virtual Vision FTP Browser Access
5084-WWW Alibaba Attack 2
5085-WWW IIS Source Fragment Access
5086-WWW WEBactive Logfile Access
5087-WWW Sun Java Server Access
5088-WWW Akopia MiniVend Access
5089-WWW Big Brother Directory Access
5090-WWW FrontPage htimage.exe Access
5091-WWW Cart32 Remote Admin Access
5092-WWW CGI-World Poll It Access
5093-WWW PHP-Nuke admin.php3 Access
5095-WWW CGI Script Center Account Manager Attack
5096-WWW CGI Script Center Subscribe Me Attack

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1245
Doc: 3690

5097-WWW FrontPage MS-DOS Device Attack
5099-WWW GWScripts News Publisher Access
5100-WWW CGI Center Auction Weaver File Access
5101-WWW CGI Center Auction Weaver Attack
5102-WWW phpPhotoAlbum explorer.php Access
5103-WWW SuSE Apache CGI Source Access
5104-WWW YaBB File Access
5105-WWW Ranson Johnson mailto.cgi Attack
5106-WWW Ranson Johnson mailform.pl Access
5107-WWW Mandrake Linux /perl Access
5108-WWW Netegrity Site Minder Access
5109-WWW Sambar Beta search.dll Access
5110-WWW SuSE Installed Packages Access
5111-WWW Solaris Answerbook 2 Access
5112-WWW Solaris Answerbook 2 Attack
5113-WWW CommuniGate Pro Access
5114-WWW IIS Unicode Attack
5115-Netscape Enterprise Server with ?wp Tags
5116-Endymion MailMan Remote Command Execution
5117-phpGroupWare Remote Command Exec
5118-eWave ServletExec 3.0C File Upload
5119-CGI Script Center News Update Admin Passwd Change
5120-Netscape Server Suite Buffer Overflow
5121-iPlanet .shtml Buffer Overflow
5122-Nokia IP440 Denial of Service
5123- WWW IIS Internet Printing Overflow
5124-IIS CGI Double Decode
5125-PerlCal Directory Traversal
5126-WWW IIS .ida Indexing Service Overflow
5127-WWW viewsrc.cgi Directory Traversal
5128-WWW nph-maillist.pl Cmd Exec
5129-IOS HTTP Unauth Command Execution
5130-Bugzilla globals.pl
5131-talkback.cgi Directory Traversal
5132-VirusScan catinfo Buffer Overflow
5133-Net.Commerce Macro Path Disclosure
5134-MacOS PWS DoS
5138-Oracle Application Server Shared Library Overflow
5140-Net.Commerce Macro Denial of Service
5141-NCM content.pl SQL Query Vulnerability
5142-DCShop File Disclosure
5143-Microsoft Media Player ASX Overflow
5146-MS-DOS Device Name DoS
5147-Arcadia Internet Store Directory Traversal Attempt
5148-Perception LiteServe Web Server CGI Script Source Code Disclosu

5149-Trend Micro Interscan Viruswall Configuration Modification
5150-InterScan VirusWall RegGo.dll Buffer Overflow
5151-WebStore Admin Bypass
5152-WebStore Command Exec
5154-WWW uDirectory Directory Traversal
5155-WWW SiteWare Editor Directory Traversal
5156-WWW Microsoft fp30reg.dll Overflow
5157-Tarantella TTAWebTop.CGI Directory Traversal Bug
5158-iPlanet Proprietary Method Overflow
5159-phpMyAdmin Cmd Exec
5160-Apache ? indexing file disclosure bug
5160:1-Apache ? indexing file disclosure bug
5161-SquirrelMail Command Exec
5162-Active Classifieds Command Exec
5163-Mambo SiteServer Administrative Password ByPass

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1246
Doc: 3690

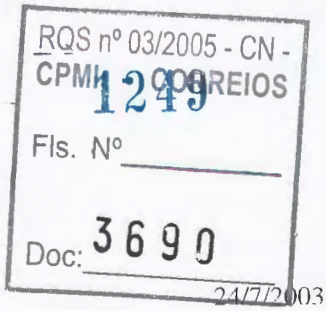
5164-PHPBB Remote SQL Query Manipulation
5165-php-nuke article.php sql query
5166-php-nuke modules.php DoS
5167-phpMyAdmin Cmd Exec 2
5168-Snapstream PVS Directory Traversal Bug
5169-SnapStream PVS Plaintext Password Vulnerability
5170-NULL byte in URI
5171-NC-Book book.cgi Cmd Exec
5172-WinWrapper Admin Server Directory Traversal
5173-Directory Manager Cmd Exec
5174-phpmyexplorer directory traversal
5175-Hassan Shopping Cart Command Exec
5176-Exchange Address List Disclosure
5178-MS Index Server File/Path Recon
5179-PHP-Nuke File Upload
5180-sgiMerchant Directory Traversal
5181-MacOS Apache File Disclosure
5181:1-MacOS Apache File Disclosure
5182-WebDiscount's eShop Arbitrary Command Exec
5183-PHP File Inclusion Remote Exec
5184-Apache Authentication Module ByPass
5188-HTTP Tunneling
5191-Active Perl PerlIS.dll Buffer Overflow
5194-Apache Server .ht File Access
5195-AS/400 '/' attack
5196-Red Hat Stronghold Recon attack
5197-Network Query Tool command Exec
5199-W3Mail Command Exec
5200-IIS Data Stream Source Disclosure
5201-PHP-Nuke Cross Site Scripting
5202- PHP-Nuke File Copy / Delete
5203- Hosting Controller File Access and Upload
5204-AspUpload Sample Scripts
5205-Apache php.exe File Disclosure
5206-Horde IMP Session Hijack
5207-Entrust GetAccess directory traversal
5208-Network Tools shell metacharacters
5209-Agora.cgi Cross Site Scripting
5210-FAQManager.cgi directory traversal
5211-zml.cgi File Disclosure
5212-Bugzilla Admin Authorization Bypass
5213-Bugzilla Command Exec
5214-FAQManager.cgi null bytes
5215-lastlines.cgi cmd exec/traversal
5216-PHP Rocket Directory Traversal
5217-Webmin Directory Traversal
5218-Boozt Buffer Overflow
5219-Lotus Domino database DoS
5220-CSVForm Remote Command Exec
5221-Hosting Controller Directory Traversal
5223-Pi3Web Buffer Overflow
5224-SquirrelMail SquirrelSpell Command Exec
5227- AHG Search Engine Command Exec
5229- DCP Portal Root Path Disclosure
5230- Lotus Domino Authentication Bypass
5231- MRTG Directory Traversal
5232-URL with XSS
5233-PHP fileupload Buffer Overflow
5234-pforum sql-injection
5236-Xoops sql-injection
5237-HTTP CONNECT Tunnel

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1247
3690
Doc:

5238-EZNET Ezboard Buffer Overflow
5239-Sambar cgitest.exe Buffer Overflow
5240-Marcus Xenakis Shell Command Exec
5241-Avenger System Command Exec
5243-CS .cgi Script Cmd Exec
5244- PhpSmsSend Command Exec
5245- HTTP 1.1 Chunked Encoding Transfer
5246-IIS ISAPI Filter Buffer Overflow
5247-IIS ASP SSI Buffer Overflow
5248-IIS HTR ISAPI Buffer Overflow
5249-IDS Evasive Encoding
5250-IDS Evasive Double Encoding
5251-Allaire JRun // Directory Disclosure
5252-Allaire JRun Session ID Recon
5253-Axis StorPoint CD Authentication Bypass
5254-Sambar Server CGI Dos Batch File
5255-Linux Directory traceroute / nslookup Command Exec
5256-Dot Dot Slash in URI
5257-PHPNetToolpack traceroute Command Exec
5258-Script source disclosure with CodeBrws.asp
5259-Snitz Forums SQL injection
5260-Xpede sprc.asp SQL Injection
5261-BackOffice Server Web Administration Access
5262-Large number of Slashes URL
5263-ecware.exe Access
5265-RedHat cachemgr.cgi Access
5266-iCat Carbo Server File Disclosure
5268-Cisco Catalyst Remote Command Execution
5269-ColdFusion CFDOCS Directory Access
5270-EZ-Mall order.log File Access
5271-search.cgi Directory Traversal
5272-count.cgi GIF File Disclosure
5273-Bannermatic Sensitive File Access
5274-Netpad.cgi Directory Traversal/Cmd Exec
5275-Phorum Remote Cmd Exec
5276-cart.cgi Command Execution
5276:1-cart.cgi vars,env,db Recon
5276:2-cart.cgi Backdoor
5277- dfire.cgi Command Exec
5278-VP-ASP shoptest.asp access
5279-JJ CGi Cmd Exec
5280-IIS idq.dll Directory Traversal
5281-Carello add.exe Access
5282-IIS ExAir advsearch.asp Access
5282:1-IIS ExAir search.asp Access
5282:2-IIS ExAir query.asp Access
5283-info2www CGI Directory Traversal
5284- IIS webhits.dll Directory Traversal
5285-PHPEventCalendar Cmd Exec
5286-WebScripts WebBBS Cmd Exec
5287-SiteServer AdSamples SITE.CSC File Access
5288-Verity search97 Directory Traversal
5289-SQLXML ISAPI Buffer Overflow
5290-Apache Tomcat DefaultServlet File Disclosure
5291-WEB-INF Dot File Disclosure
5292-SalesCart shop.mdb File Access
5293-robots.txt File Access
5294-BearShare File Disclosure
5295-finger CGI Recon
5296-Netscape Server PageServices Directory Access
5297-order_log.dat File Access

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 1248
Doc: 3690

5298-shopper.conf File Access
5299-quikstore.cfg File Access
5300-reg_echo.cgi Recon
5301-/consolehelp/ CGI File Access
5302-/file/ WebLogic File Access
5303-pfdispaly.cgi Command Execution
5304-files.pl File Access
5305-.bash_history File Access
5305:1-.sh_history File Access
5305:2-.history File Access
5305:3-.zhistory File Access
5306-SoftCart storemgr.pw File Access
5308-rpc-nlog.pl Command Execution
5309- handler CGI Command Execution
5310-INDEX / directory access
5311-8.3 file name access
5312-*.jsp/*.jhtml Java Execution
5313-order.log File Access
5314- windmail.exe Command Execution
5315-changedisplay.pl WWWthreads Privilege Elevation
5316-BadBlue Admin Command Exec
5317-Tivoli Endpoint Buffer Overflow
5318-Tivoli ManagedNode Buffer Overflow
5319-SoftCart orders Directory Access
5320-ColdFusion administrator Directory Access
5321-Guest Book CGI access
5322-Long HTTP Request
5323-Cisco Router http exec command
5323-midicart.mdb File Access
5324-Cisco IOS Query (?/)
5325-Contivity cgiproc DoS
5326-Root.exe access
5327-Tilde in URI
5328- Cisco IP phone DoS
5329-Apache/mod_ssl Worm Probe
5330-Apache/mod_ssl Worm Buffer Overflow
5331-Image Javascript insertion
5332-Wordtrans-web Command Exec
5333-FUDForum File Disclosure
5334- DB4Web File Disclosure
5335-DB4WEB Proxy Scan
5336- Abyss Web Server File Disclosure
5337-Dot Dot Slash in HTTP Arguments
5338-Front Page Admin password retrival
5339-SunONE Directory Traversal
5340-Killer Protection Credential File Access
5341-HP Procurve 4000M Switch DoS
5342-Invision Board phpinfo.php Recon
5343-Apache Host Header Cross Site Scripting
5344-IIS MDAC RDS Buffer Overflow
5345-HTTPBench Information Disclosure
5346-BadBlue Information Disclosure
5347-Xoops WebChat SQL Injection
5348-Cobalt RaQ Server overflow.cgi Cmd Exec
5349-Polycom ViewStation Admin Password
5350-PHPnuke email attachment access
5351-MS IE Help Overflow
5352-H-Sphere Webshell Buffer Overflow
5353-H-Sphere Webshell 'mode' URI exec
5354-H-Sphere Webshell zipfile' URI exec
5355-DotBr exec.php3 exec



5356-DotBr system.php3 exec
5357-IMP SQL Injection
5358-Psunami.CGI Remote Command Execution
5359-Office Scan CGI Scripts Access
5360-Frontpage htimage.exe Buffer Overflow
5362-FrontPage dvwssr.dll Buffer Overflow
5363-Frontpage imagemap.exe Buffer Overflow
5364-IIS WebDAV Overflow
5365-Long WebDAV Request
5366-Shell Code in HTTP URL / Args
5367-Apache CR / LF DoS
5368-Cisco ACS Windows CSAdmin Overflow
5369-Win32 Apache Batch File CmdExec
5370-HTDig File Disclosure
5371-bdir.htr Access
5372-ASP %20 source disclosure
5373-IIS 5 Translate: f Source Disclosure
5374-IIS Executable File Command Exec
5381-VPASP SQL injection
6001-Normal SATAN Probe
6002-Heavy SATAN Probe
6050-DNS HINFO Request
6051-DNS Zone Transfer
6052-DNS Zone Transfer from High Port
6053-DNS Request for All Records
6054-DNS Version Request
6055-DNS Inverse Query Buffer Overflow
6056-DNS NXT Buffer Overflow
6057-DNS SIG Buffer Overflow
6058-DNS SRV DoS
6059-DNS TSIG Overflow
6060-DNS complain overflow
6061-DNS infoleak
6062-DNS authors request
6063-DNS Incremental zone transfer
6064-BIND Large OPT Record DoS
6100-RPC Port Registration
6101-RPC Port Unregistration
6102-RPC Dump
6103-Proxied RPC Request
6104-RPC Set Spoof
6105-RPC Unset Spoof
6110-RPC RSTATD Sweep
6111-RPC RUSERSD Sweep
6112-RPC NFS Sweep
6113-RPC MOUNTD Sweep
6114-RPC YPPASSWDD Sweep
6115-RPC SELECTION_SVC Sweep
6116-RPC REXD Sweep
6117-RPC STATUS Sweep
6118-RPC ttdb Sweep
6150-ypserv Portmap Request
6151-ypbind Portmap Request
6152-yppasswdd Portmap Request
6153-ypupdated Portmap Request
6154-ypxfrd Portmap Request
6155-mountd Portmap Request
6175-rexd Portmap Request
6180-rexd Attempt
6188-statd dot dot
6189-statd automount attack

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1250
Doc: 3690

6190-statd Buffer Overflow
6191-RPC.tooltalk buffer overflow
6192-RPC mountd Buffer Overflow
6193-RPC CMSD Buffer Overflow
6194-sadmind RPC Buffer Overflow
6195-RPC amd Buffer Overflow
6196-snmpXdmid Buffer Overflow
6197-rpc yppaswdd overflow
6198-rwalld String Format
6199-cachefsd Overflow
6200-Ident Buffer Overflow
6201-Ident Newline
6210-LPRng format String Overflow
6250-FTP Authorization Failure
6251-Telnet Authorization Failure
6252-Rlogin Authorization Failure
6253-POP3 Authorization Failure
6255-SMB Authorization Failure
6275-SGI fam Attempt
6276-TooltalkDB overflow
6277-Show Mount Recon
6300-Loki ICMP Tunneling
6302-General Loki ICMP Tunneling
6350-SQL Query Abuse
6500-RingZero Trojan
6501-TFN Client Request
6502-TFN Server Reply
6503-Stacheldraht Client Request
6504-Stacheldraht Server Reply
6505-Trinoo Client Request
6506-Trinoo Server Reply
6507-TFN2K Control Traffic
6508-Mstream Control Traffic
6901-Net Flood ICMP Reply
6902-Net Flood ICMP Request
6903-Net Flood ICMP Any
6910-Net Flood UDP
6920-Net Flood TCP
7101-ARP Source Broadcast
7102-ARP Reply-to-Broadcast
7104-ARP MacAddress-Flip-Flop-Response
7105-ARP Inbalance-of-Requests
8000:2101-FTP Retrieve Password File
8000:2302-Telnet-/etc/shadow Match
8000:2303-Telnet-+ +
8000:51301-Rlogin-IFS Match
8000:51302-Rlogin-/etc/shadow Match
8000:51303-Rlogin-+ +
9000-Back Door Probe (TCP 12345)
9001-Back Door Probe (TCP 31337)
9002-Back Door Probe (TCP 1524)
9003-Back Door Probe (TCP 2773)
9004-Back Door Probe (TCP 2774)
9005-Back Door Probe (TCP 20034)
9006-Back Door Probe (TCP 27374)
9007-Back Door Probe (TCP 1234)
9008-Back Door Probe (TCP 1999)
9009-Back Door Probe (TCP 6711)
9010-Back Door Probe (TCP 6712)
9011-Back Door Probe (TCP 6713)
9012-Back Door Probe (TCP 6776)

RQS nº 03/2005 - CN - CPMI - CORREIOS
1251
Fls. Nº
Doc: 3690

9013-Back Door Probe (TCP 16959)
9014-Back Door Probe (TCP 27573)
9015-Back Door Probe (TCP 23432)
9016-Back Door Probe (TCP 5400)
9017-Back Door Probe (TCP 5401)
9018-Back Door Probe (TCP 2115)
9019-Back Door (UDP 2140)
9020-Back Door (UDP 47262)
9021-Back Door (UDP 2001)
9022-Back Door (UDP 2002)
9023-Back Door Probe (TCP 36794)
9024-Back Door Probe (TCP 10168)
9025-Back Door Probe (TCP 20168)
9026-Back Door Probe (TCP 1092)
9027-Back Door Probe (TCP 2018)
9028-Back Door Probe (TCP 2019)
9029-Back Door Probe (TCP 2020)
9030-Back Door Probe (TCP 2021)
9200-Back Door Response (TCP 12345)
9201-Back Door Response (TCP 31337)
9202-Back Door Response (TCP 1524)
9203-Back Door Response (TCP 2773)
9204-Back Door Response (TCP 2774)
9205-Back Door Response (TCP 20034)
9206-Back Door Response (TCP 27374)
9207-Back Door Response (TCP 1234)
9208-Back Door Response (TCP 1999)
9209-Back Door Response (TCP 6711)
9210-Back Door Response (TCP 6712)
9211-Back Door Response (TCP 6713)
9212-Back Door Response (TCP 6776)
9213-Back Door Response (TCP 16959)
9214-Back Door Response (TCP 27573)
9215-Back Door Response (TCP 23432)
9216-Back Door Response (TCP 5400)
9217-Back Door Response (TCP 5401)
9218-Back Door Response (TCP 2115)
9223-Back Door Response (TCP 36794)
9224-Back Door Response (TCP 10168)
9225-Back Door Response (TCP 20168)
9226-Back Door Response (TCP 1092)
9227-Back Door Response (TCP 2018)
9228-Back Door Response (TCP 2019)
9229-Back Door Response (TCP 2020)
9230-Back Door Response (TCP 2021)
10000:1000-IP-Spoof Interface 1
10000:1001-IP-Spoof Interface 2
11000-KaZaA v2 UDP Client Probe
11001-Gnutella Client Request
11002-Gnutella Server Reply
11003-Qtella File Request
11004-Bearshare file request
11005-KaZaA GET Request
11006-Gnucleus file request
11007-Limewire File Request
11008-Morpheus File Request
11009-Phex File Request
11010-Swapper File Request
11011-XoloX File Request
11012-GTK-Gnutella File Request
11013-Mutella File Request

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1252
3690
Doc:

11014-Hotline Client Login
11015-Hotline File Transfer
11016-Hotline Tracker Login
11200-Yahoo Messenger Activity
11201-MSN Messenger Activity
11202-AOL / ICQ Activity
11203- IRC Channel Join

BUSINESS STRATEGIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | PRODUCTS & SERVICES | TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESELLERS | ABOUT CISCO
Home | Logged In | Profile | Contacts & Feedback | Site Help
© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1253
Doc: 3690

Manual 1

IBM TotalStorage TM
SAN Swtich M12

ROS nº 03/2005 - C.J. -
CPMI - CORREIOS
1254
Fls. Nº
Doc: 3690

Core fabric switch supports highly scalable fabrics for large enterprise SANs

IBM TotalStorage™ SAN Switch M12

High port density packaging saves space

Highlights

- ***Designed to provide superior performance with up to 2 Gbit/sec throughput and Inter-Switch Link (ISL) Trunking with aggregate speed up to 8 Gbit/sec***
- ***Enterprise-level scalability and high availability when deployed with dual redundant core/edge fabrics capable of attaching thousands of devices***
- ***Scalable from one 32-port swtich to two 64-port switches***
- ***Broadest range of IBM open server and storage device attachment including fabric, public loop and private loop with QuickLoop enabled edge switches***
- ***Space saving Small Form-Factor Pluggable (SFP) transceivers with up to 128-ports of Fibre Channel connectivity in 14U enclosure***
- ***Advanced fabric services such as end-to-end performance monitoring***
- ***Multiple SAN management options include IBM TotalStorage SAN Switch Specialist, Fabric Manager V3 and open fabric interfaces for centralized management of large core/edge fabrics***

IBM TotalStorage Enterprise SAN products

The IBM TotalStorage enterprise Storage Area Network (SAN) products create a high-speed, interconnected switch fabric of centrally managed, multi-vendor heterogeneous servers and storage systems. An enterprise SAN built upon IBM SAN technology can help companies derive greater value from their business information by supporting improved IT resource management and information sharing across the enterprise.

IBM TotalStorage SAN Switch M12

The IBM TotalStorage SAN Switch M12 (M12 Switch) provides 2 Gbit Fibre Channel capability and performance and advanced functions to address demands for improved security, performance and manageability as the SAN fabric grows to include thousands of devices. It is based on next-generation switch technology that is designed to help full interoperable with other IBM TotalStorage SAN Switches. You can configure scalable solutions that address your needs for high performance and reliability for environments ranging from small workgroups to very large, integrated enterprise SANs.

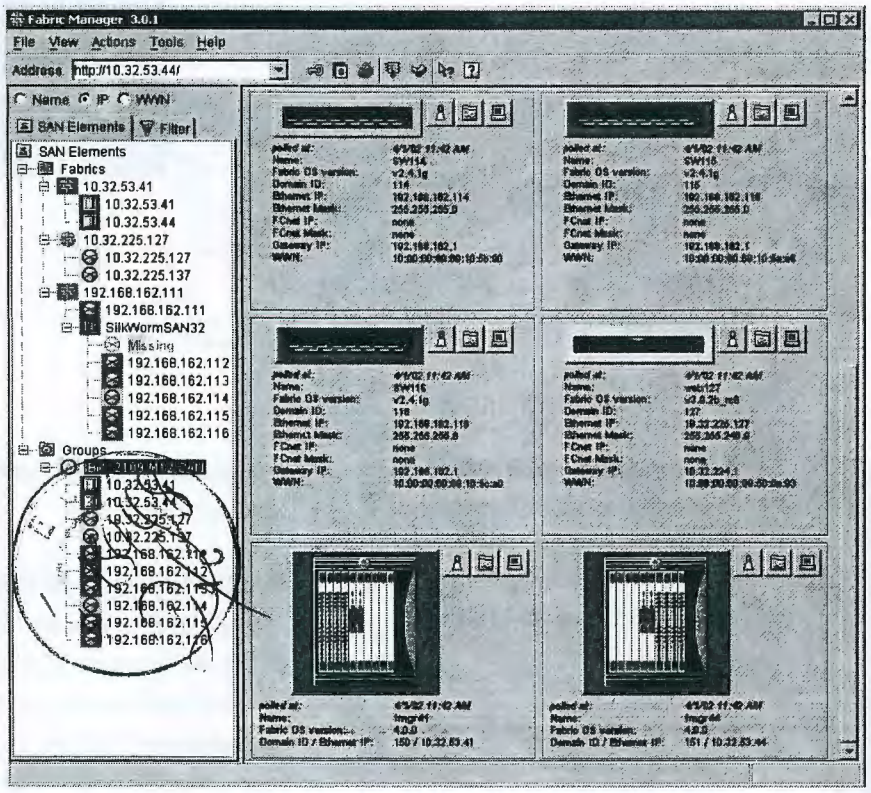
Industry-standard Fibre Channel

The M12 Switch is designed to provide Fibre Channel connectivity to:

Servers:

- *IBM @server pSeries and selected RS/6000 servers (for the most current list of supported servers and storage, visit ibm.com/storage/FCSwitch)*
- *IBM @server xSeries and selected Netfinity servers*
- *Other Intel®-based servers with Windows NT®/2000*

ECT 06/2003 - CN - CPMI - CORREIOS
Fls. Nº 1255
Doc: 3690



SAN Switch Specialist Switch View

Storage Systems

- *IBM Enterprise Storage Server®*
- *IBM FAStT Storage Server® family*
- *IBM 3590 Tape Subsystems and 3494 Tape Libraries*
- *IBM 3583 and 3584 Ultrium Tape Libraries*

SAN Switches

- *IBM TotalStorage SAN Switch F16 and F08 (F16 and F08 Switches)*
- *IBM TotalStorage SAN Switch S16, S08 (S16 and S08 Switches) and IBM TotalStorage SAN Managed Hub*

The M12 Switch supports the interconnection of multiple IBM SAN Switches. The interconnection of IBM and compatible (Brocade® SilkWorm® 2400, 2800, 3200, 3800 and 12000) switches can support the creation of a scalable, dual redundant core-to-edge SAN fabrics that can support high performance, scalability, and fault tolerance required e-business applications and enterprise storage management applications—such as storage consolidation, data protection, disaster tolerance and data sharing.

IBM TotalStorage SAN Switches

IBM S08 and S16 Switches are designed to support ANSI-standard Fibre Channel protocol at 1 Gbit/sec. The M12 Switch is built upon a next-generation switch technology that provides link speeds of 1 and 2 Gbit/sec. Each port supports either 100MB/sec or 200MB/sec, full-duplex data transfers. Auto-sensing ports are capable of automatically negotiating to the highest speed supported by the attached server, storage or switch.

The M12 Switch is suited for disaster tolerance solutions such as remote tape vaulting and remote disk mirroring. M12 Switches can provide up to twice the throughput of S16 Switches. This performance capability can be used to either reduce the number of expensive extended distance ISL connections or to improve the performance with the same number of connections.

M12 Switches can be combined with F16 and F08 Switches to provide fabrics up to twice the performance of S16 and S08 Switch fabrics. Customers can deploy M12 Switches that are ready to exploit the performance potential of newer servers and storage devices with 2 Gbit/sec capabilities.

M12 Switches can be used to expand an existing core-to-edge SAN fabric infrastructure. As M12 Switches are added to the core, installed F16, S16 and S08 Switches can be migrated to the edge. This approach helps support scalable network growth in a modular, cost effective and non-disruptive manner while customers continue to derive benefit from installed switches.

Common SAN Switch functions and features

IBM TotalStorage SAN Switches include universal ports that can automatically determine the port type when connected to a fabric port (F_port), fabric loop port (FL_port) or expansion port (E_port). Fabric services include automatic self-discovery of new devices and dynamic path selection based upon Fabric Shortest Path First (FSPF) which is designed to select the most efficient routing in a SAN fabric. A mixture of shortwave and longwave ports can be configured. The core fabric switch is designed to provide improved switch availability with hot swappable components that can be replaced or upgraded without interrupting network operations. Components include switch modules, redundant power supplies, cooling systems and processors and support for non-disruptive software upgrades.

Common firmware functions and features

The common IBM SAN Switch firmware simplifies SAN fabric expansion. Standards-based Management Server and Simple Name Server support in-band discovery of SAN fabric changes. Management access of SNMP information is provided via an external Ethernet interface or in-band over a Fibre Channel link through a single fabric connection.

Device-level zoning of the SAN fabric enables an administrator to create separate segments or zones within the SAN fabric to separate different application servers and devices in heterogeneous SAN environments. Zones may be dynamically created and changed from any switch in the fabric. Basic security functions such as hardware-enforced zoning are standard.

Extended Fabric Activation extends SAN fabrics beyond the Fibre Channel standard 10 km. This enables high performance applications over extended distances for storage consolidation, data protection, disaster tolerance and data sharing. ISLs using extended longwave transceivers, Fibre Channel repeaters and Dense Wave Division Multiplexing (DWDM) devices can provide Metropolitan Area Network (MAN) connectivity distances. Extended Fabrics Activation helps optimize switch buffering to support high gateway switch ISL performance.

Remote Switch Activation extends the distance of SAN fabrics by enabling two Fibre Channel switches to interconnect over an ATM Wide Area Network (WAN). With this feature, one can stage and manage data transfers across a pair of Fibre Channel switches connected to a pair of CNT Open System Gateways.

QuickLoop enables servers with Fibre Channel Arbitrated Loop (FC-AL) private loop Host Bus Adapters (HBAs) to communicate with FC-AL storage devices through IBM SAN Switches. The M12 Switch does not provide QuickLoop capability. However, IBM SAN Switches with QuickLoop enabled may be used to attach private loops devices to M12 Switches.

M12 Switch configuration options

A single switch with two 16-port switch blades and thirty-two universal ports, is scalable up to two 64-port switches, each with four switch blades. A mixture of shortwave and longwave ports can be configured by adding up to 128 SFP optical transceivers.

Inter-Switch Link (ISL) Trunking, a standard feature, enables as many as four Fibre Channel links between next-generation switch technology M12, F16 and F08 Switches to be combined to form a single logical ISL with an aggregate speed of up to 8 Gbit/sec. These high-speed trunks help optimize bandwidth utilization and enhance availability.

Load balancing can help balance the load across all of the ISLs through trunking. This enables administrators to focus on overall network performance rather than individual link congestion from multiple higher performance devices sharing a single link. Administrators need only to monitor the trunk performance rather than specific devices being routed across it. Increased network reliability and performance is supported because failed links do not require rerouting of traffic.

End-to-end performance monitoring

Next-generation switching technology enables Frame Filtering, which is based upon additional information in several fields in both the packet header and payload. Frame Filtering enables new intelligent fabric services such as end-to-end performance analysis.

S08 and S16 Switches provide performance information at the switch or port level. M12 Switches with Frame Filtering provide detailed information at the frame level. This information can be used to monitor performance end-to-end across the entire core-to-edge SAN fabric—from a specific server to a specific storage device port.

Performance Monitoring, a standard feature, provides support for Frame Filtering-based Performance Monitoring tools for enhanced end-to-end performance monitoring. As core-to-edge SAN fabrics scale up to thousands of devices, ISL Trunking and Frame Filtering can help to simplify storage management and reduce the overall cost of the storage infrastructure.

C36 Cabinet options

The C36 Cabinet is based upon a standard 19-inch rack, and offers 36U vertical space. It is specifically designed to support two M12 Switches with two power distribution units, each with three power outlets. A Ruggedized Rack feature provides enhanced rigidity and stability for locations with earthquake concerns.

Open fabric management

IBM SAN Switch management framework is designed to support the widest range of solutions—from the very small workgroup SANs up to very large enterprise SAN fabrics with thousands of devices. Small SANs require rapid deployment and plug-and-play simplicity. Very large SAN fabrics require centralized management and automated administration. IBM SAN Switch

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 1256
Doc: 3690

IBM TotalStorage SAN Switch M12 at a glance

Physical characteristics	M12 Switch	C36 Cabinet
Height	61.24 cm/24.11 in (14U)	180.4 cm/71.0 in (36U)
Width	43.74 cm/17.22 in	64.4 cm/25.4 in
Depth	74.20 cm/29.20 in	109.8 cm/43.3 in
Weight (fully populated)	113 kg/248 lb	One M12 357 kg/784 lb Two M12s 470 kg/1032 lb
Operating environment		
Temperature	0° to 40 ° C/32° to 104° F	10° to 40 ° C/50° to 104° C
Relative humidity	20% to 85% at 40° C/104° F	8% to 80% at 40° C/104° F
Power requirements		
Power range	180 to 264 VAC, 47 to 63 Hz	200 to 240 VAC, 50-60 Hz

Product numbers

2109 M12—IBM TotalStorage SAN Switch M12, a 32-port core fabric switch with enclosure includes four power supplies, three fans, two control processors and two 16-port, 2 Gb switch blades. The base configuration includes Fabric OS Version 4.0, IBM SAN Switch Specialist, Advanced Zoning, FabricWatch, ISL-Trunking, Performance Monitoring and space for two 64-port switches.
FC 2310—M12 Shortwave SFP transceiver
FC 2320—M12 Longwave SFP transceiver
FC 3216—16 Port Switch Blade

Fiber Optic Cables:
FC 5301—M12 Fiber cable, LC/LC, multimode optical, 50.0u, 1 meters
FC 5305—M12 Fiber cable, LC/LC, multimode optical, 50.0u, 5 meters
FC 5325—M12 Fiber cable, LC/LC, multimode optical, 50.0u, 25 meters
FC 5371—M12 Fiber LC/SC (male/female) coupling cable, multimode optical, 50.0u, 1 meters
FC 5372—M12 Fiber LC/SC (male/female) coupling cable, multimode optical, 50.0u, 2 meters

Advanced Fabric Features:
FC 7301—Fabric Manager V3
FC 7602—Remote Switch Activation
FC 7603—Extended Fabric Activation

2109 C36—IBM TotalStorage SAN Cabinet C36, 19-inch rack with 36U space, designed to support two M12 Switches with two power distribution units, each with three power outlets.
FC 6080—Ruggedized Rack

management options include a browser-based IBM TotalStorage SAN Switch Specialist, Fabric Manager V3 and open standards-based interfaces to enterprise SAN managers.

IBM TotalStorage SAN Switch Specialist is designed to provide a comprehensive set of management tools that support a Web browser interface for flexible, easy-to-use integration into existing enterprise storage management structures. The Switch Specialist supports security and data integrity by limiting (zoning) host system attachment to specific storage systems and devices.

Fabric Watch is a standard function on M12, F16, F08 (Full-Fabric), S16* and S08* Switches. Fabric Watch threshold monitoring tracks the health of switches and SAN fabric. Fabric Watch monitors fabric resources, port traffic, switch environmental values and operational values for GigaBit Interface Converters (GBIC) and optical transceivers. This information is accessible from the Switch Specialist. When used with M12 Switches, the Specialist provides an easy-to-use interface to intelligent fabric features such as end-to-end performance monitoring and ISL Trunking.

Fabric Manager V3 provides a Java-based application that can simplify management of a complex, multiple switch fabrics. IBM SAN Switch Specialist and Fabric Manager work together on the same management server which can be attached to any switch in the core/edge fabric. It may also manage up to eight separate fabrics. Fabric Manager requires a Windows NT/2000 or Sun Solaris 7 server with a Netscape or Internet Explorer web browser.

Enterprise SAN fabric management

Fabric Watch can send alerts to enterprise SAN fabric management software from vendors such as Computer Associates, Hewlett Packard, Tivoli, and VERITAS. Brocade Fabric Access Layer API server agents are available on IBM SAN Switches. Only a single connection to the fabric is required to access any switch or fabric-wide resource.

For more information

For more information, contact your IBM representative or IBM Business Par
Or visit **ibm.com**/storage/FCSwitch.

© International Business Machines Corporation 2002

IBM Corporation
Storage Systems Group
5600 Cottle Road
San Jose, CA 95193

Produced in the United States of America
05-02
All Rights Reserved

* Models S08 and S16 shipped after March 23, 2001.

IBM and the IBM logo, Enterprise Storage Server, @server, Magstar, Netfinity, RS/6000, and S/390, are registered trademarks and iSeries, p5, TotalStorage, xSeries, and zSeries are trademarks of International Business Machines Corporation.

Windows 2000 and Windows NT are trademarks of Microsoft Corporation in the United States, other countries or both. UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

G225-6946-01

Manual 02

IBM TotalStorage TM
SAN Fibre Channel Switch 2109 M12

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1257
Doc: 3690

IBM TotalStorage ™ SAN Fibre Channel Switch 2109 Model M12

IBM Storage and Server Interoperability Matrix

Last update: Jun. 18, 03

© Copyright International Business Machines Corporation 1999, 2003. All rights reserved.

The information provided in this document is provide "AS IS" without warranty of any kind, including any warranty of merchantability, fitness for a particular purpose, interoperability or compatibility. IBM's products are warranted in accordance with the agreements under which they are provided.

Unless otherwise specified, the product manufacturer, supplier, or publisher of non-IBM products provides warranty, service, and support directly to you. IBM makes no representations or warranties regarding non-IBM products.

The inclusion of an IBM or non-IBM product on an interoperability list is not a guarantee that it will work with the designated IBM storage product. In addition, not all software and hardware combinations created from compatible components will necessarily function properly together. The following list includes products developed or distributed by companies other than IBM. IBM does not provide service or support for the non-IBM products listed, but does not prohibit them from being used together with IBM's storage products. During problem debug and resolution, IBM may require that hardware or software additions be removed from the IBM product to provide problem determination and resolution on the IBM-supplied hardware/ software. For support issues regarding non-IBM products, please contact the manufacturer of the product directly. IBM does not warrant either functionality or problem resolution of any non-IBM products.

This information could include technical inaccuracies or typographical errors. IBM does not assume any liability for damages caused by such errors as this information is provided for convenience only; the reader should confirm any information contained herein with the associated vendor.

Changes are periodically made to the content of the document. These changes will be incorporated in new editions of the document. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this document at anytime without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

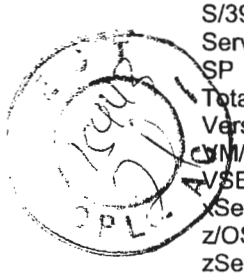
All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

RQS nº 03/2003 - CN - CPMI - CORREIOS
Fls. Nº 1258
Doc: 3690

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX
AS/400
DYNIX
DYNIX/ptx
e (logo)
Enterprise Storage Server
ESCON
ES/9000
FICON
FlashCopy
IBM
IBM logo
iSeries
Micro Channel
Multiprise
Netfinity
NUMA-Q
OS/390
OS/400
PTX
pSeries
Redbooks
RS/6000
S/390
S/390 Parallel Enterprise Server
SP
TotalStorage
Versatile Storage Server
VM/ESA
VSE/ESA
xSeries
z/OS
zSeries
z/VM



Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Table of Contents

ESS
FAStT
Tape

Notes:

1. Firmware version **4.1.0** or later and Fabric Manager **4.0** are recommended.
2. Reference Information.
3. Advanced Security Feature is available with firmware version 4.1.0 or later.
4. Secure Fabric OS - Field Upgrade Process. (Hints and Tips).
5. SAN Fibre Channel Switch 2109 Model M12 Data Sheet (pdf).
6. Both tape and disk attached to the same HBA are not recommended.
7. We do not recommend attaching the NAS 300G *to* an **unzoned** switch configuration.
8. Planned availability dates represent current estimates and are subject to change or withdrawal at any time without notice.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1259
Doc: 3690

ESS Connectivity

See **IBM TotalStorage Enterprise Storage Server Interoperability Matrix** for Licensed Internal Code (LIC) level.

IBM pSeries, RS/6000 and RS/6000-SP Servers

Description	Operating Systems	Additional Information

IBM TotalStorage Enterprise Storage Servers
IBM 2105 Model
• F10/F20
• 800
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2 [1]
	
	HACMP [2]
	PSSP [2]
		Available
		
		Enterprise Storage Server Interoperability matrix
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.

[1] Planned availability is 2Q03 for RS/6000-SP with AIX 5.2.
[2] See **ESS** Interoperability matrix for **AIX, HACMP, PSSP, and SDD** support information.

IBM xSeries, Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Enterprise Storage Servers **IBM 2105 Model** • F10/F20 • 800	**Microsoft Windows NT** • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server • Datacenter Server	Available **Enterprise Storage Server** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Novell Netware • 5.1 • 6.0	Available
	Red Hat Linux • 7.1 • 7.2 • 7.3 **Red Hat Linux Advanced Server** • 2.1 **SuSE Linux** • 7.2 • 7.3 **SuSE Linux Enterprise Server (SLES)** • 7 • 8	Available
	IBM TotalStorage Network Attached Storage 300G	Available

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1260
Doc: 3690

SUN microsystems Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Enterprise Storage Servers **IBM 2105 Model** • F10/F20 • 800	**Solaris** • 2.6 • 7 • 8 • 9 [3]	Available **Enterprise Storage Server** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
IBM TotalStorage Enterprise Storage Servers **IBM 2105 Model** • F10/F20 • 800	**HP-UX** • 11.0 • 11i	Available **Enterprise Storage Server** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

[3] Solaris 9 is not supported SDD at this time.

FAStT Connectivity

1 We do not recommend attaching the **IBM FAStT** on the same Intel server as the **TotalStorage Enterprise Storage Server**. Both devices may be attached to the same switch.

2 For the most current supported **HACMP, PSSP, GPFS/RVSD** configurations see the config files posted on:
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt900downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt700downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt600downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt500downloads
- http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/fastt200downloads

3 **GPFS** Linux supported on selected **xSeries** servers running RH 7.2, 7.3 or SuSE Linux Enterprise Server 7 or 8. Refer to the **IBM** Linux and **eServer** Cluster support pages.
- http://ibm.com/servers/eserver/clusters
- http://ibm.com/linux

IBM pSeries, RS/6000 and RS/6000 SP Servers

Description	Operating Systems	Additional Information

IBM TotalStorage Storage Servers
• **FAStT900**
• **FAStT600**
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2
	
	HACMP, PSSP (see note #2 page 7)
		Available
		
		IBM TotalStorage FAStT Storage Interoperability matrix
		
		IBM Server Proven Interoperability matrix
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1261
Doc: 3690

IBM xSeries, Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • FAStT900 • FAStT600	**Microsoft Windows NT** • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Novell Netware • 6.0	Available
IBM TotalStorage Storage Servers • FAStT900	**Red Hat Linux Advanced Server** • 2.1 **SuSE Linux Enterprise Server (SLES)** • 7 • 8	Available
IBM TotalStorage Storage Servers • FAStT600	**Red Hat Linux Advanced Server** • 2.1 **SuSE Linux Enterprise Server (SLES)** • 8	Available

SUN microsystems Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT900** • **FAStT600**	**Solaris** • 2.6 • 7 • 8	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

Hewlett-Packard Servers – HP- UX

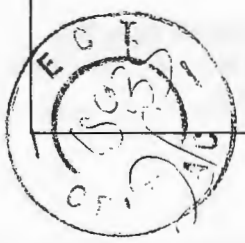
Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT900** • **FAStT600**	**HP-UX** • 11.0 • 11i	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1262
3690
Doc:

IBM pSeries, RS/6000 and RS/6000 SP Servers

Description	Operating Systems	Additional Information

IBM TotalStorage Storage Servers
• **FAStT700**
• **FAStT500**
• **FAStT200**
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2
	
	HACMP, PSSP (see note #2 page 7)
		Available
		
		IBM TotalStorage FAStT Storage Interoperability matrix
		
		IBM Server Proven Interoperability matrix
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.



IBM xSeries and Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • FAStT700 • FAStT500 • FAStT200	**Microsoft Windows NT** • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Novell Netware • 5.1 • 6.0	Available
	Red Hat Linux • 7.1 • 7.2 • 7.3 **Red Hat Linux Adv. Server** • 2.1 **SuSE Linux** •7.3 **SuSE Linux Enterprise Server** • 7 • 8 **Turbo Linux** • 7.0	Available
	IBM TotalStorage Network Attached Storage 300G	Available

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1263
Doc: 3690

SUN microsystems Servers

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT700** • **FAStT500** • **FAStT200**	**Solaris** • 2.6 • 7 • 8	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
IBM TotalStorage Storage Servers • **FAStT700** • **FAStT500** • **FAStT200**	**HP-UX** • 11.0 • 11i	Available **IBM TotalStorage** FAStT Storage Interoperability matrix **IBM Server Proven** Interoperability matrix **Fibre Channel Host Bus Adapter** firmware and driver level matrix.

TAPE Connectivity

AVOID DYNAMIC ZONING CHANGES
As a recommendation, we advise that one avoid making zoning changes to your fabric while data is being transferred, if possible. There may be some risk in job interruption, especially with serial data during the Registered State Change Notifications (RSCN's) that are produced as a result of the zone change. Some HBA's are more prone to an interruption than others.

IBM 2064 zSeries Servers

Description	Operating Systems	Additional Information
Ultrium 3584 UltraScalable Tape Library with Native FC Ultrium 2 drives only. (Feature Code 1476)	**IBM zSeries Servers Models z800 and z900** **SuSE Linux Enterprise Server 8** **FICON or FICON Express Channels** with FCP enablement firmware **Longware** • FC 2315 • FC 2319 **Shortware** • FC 2318 • FC 2320	Available **zSeries Support of Fibre Channel FCP Channels**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1264
Doc: 3690

IBM pSeries, RS/6000 and RS/6000 SP Servers

Description	Operating Systems	Additional Information

Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame.
 	
Ultrium 3584 UltraScalable Tape Library with Native FC Ultrium 1 and 2 drives.
 	
Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2 drives.
 	
Ultrium 3583 Scalable Tape Library with Integrated SDG Module.
 	
Ultrium 3582 Tape Library with Native FC Ultrium 2 drives.
	AIX
	• Version 4
	  • 4.3.3
	• Version 5
	  • 5.1
	  • 5.2
		Available
		
		Fibre Channel Host Bus Adapter firmware and driver level matrix.

IBM xSeries, Netfinity Servers and other Intel-based Servers

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 and 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives.	**Microsoft Windows NT** [4] • Server 4.0 • Server 4.0 Enterprise Edition **Microsoft Windows 2000** • Server • Advanced Server • Datacenter Server **Microsoft Windows 2003 Server** [5] • Standard Edition • Enterprise Edition • Datacenter Server • Web Edition	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
	Red Hat Advanced Server • 2.1 **SuSE Linux Enterprise Server (SLES)** • 7	Available Please review **RMSS Technical Support** Site.

[4] Windows NT 4.0 planed available on June 2003 for Ultrium 3582 Tape Library and Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2.
[5] Windows 2003 supports Ultrium 3582 Tape Library and Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2 only at this time.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1265
3690
Doc:

SUN microsystems Servers

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 drives. **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module	**Solaris** • 2.6 • 7 • 8 • 9	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix.
Ultrium 3584 UltraScalable Tape Library with Native FC Ultrium 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. [6] **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives. [7]	**Solaris** • 7 • 8 • 9	Available

[6] Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2- support available June 2003.
[7] Ultrium 3582 Tape Library with Native FC Ultrium 2- support available June 2003.

Hewlett-Packard Servers – HP- UX

Description	Operating Systems	Additional Information
Enterprise Tape System 3590 E11/E1A and H11/H1A with Native FC Tape Drives. Standalone or in a 3494 Tape Library or Silo Compatible Frame **Ultrium 3584 UltraScalable** Tape Library with Native FC Ultrium 1 and 2 drives. **Ultrium 3583 Scalable** Tape Library with Native FC Ultrium 2 drives. [8] **Ultrium 3583 Scalable** Tape Library with Integrated SDG Module **Ultrium 3582** Tape Library with Native FC Ultrium 2 drives. [9]	**HP-UX** • 11.0 • 11i	Available **Fibre Channel Host Bus Adapter** firmware and driver level matrix. For specific details and restrictions please see the **readme** file.

[8] Ultrium 3583 Scalable Tape Library with Native FC Ultrium 2- support available June 2003.
[9] Ultrium 3582 Tape Library with Native FC Ultrium 2 - support available June 2003.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1266
Fls. Nº
3690
Doc:

Manual 03

2109 Model C36 With Model M12
Installation and Service Guide

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1267
Doc: 3690

IBM TotalStorage SAN Cabinet

2109 Model C36 with Model M12 Installation and Service Guide

Read Before Using

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1268
Fls. Nº
3690
Doc:

GC26-7467-03

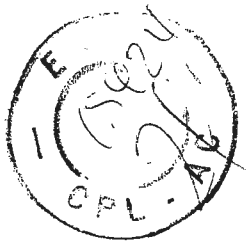
IBM TotalStorage SAN Cabinet

2109 Model C36 with Model M12 Installation and Service Guide

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1269
Doc: 3690

GC26-7467-03

Note:
Before using this information and the product it supports, read the general information in "Safety and environmental notices" on page xi, and "Notices" on page 123.



Fourth Edition (May 2003)

This edition replaces GC26-7467-02.

© Copyright International Business Machines Corporation 2002, 2003. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables ix

Safety and environmental notices xi
Safety notices xi
Safety inspection procedures xi
Inspecting the cabinet. xi
Inspecting the 2109 Model M12 xiv
Inspecting the bridge tool xviii
Environmental notices and statements xxi
Laser safety xxi
Battery notice xxii
Fire suppression systems. xxii
Product recycling xxii
Product disposal xxii

About this document xxiii
Who should read this document xxiii
Additional information xxiii
2109 Model C36 with Model M12 library xxiii
Related documents xxiii
Web sites xxiv
Getting help xxiv
Getting software updates. xxiv
How to send your comments xxv

Chapter 1. Introduction 1
Overview 1
Software features 2
Port side of chassis 3
Blower assembly side of chassis 4
Monitoring and managing the 2109 Model M12 4

Chapter 2. Installing the 2109 Model C36 7
Step 1. Position the cabinet. 7
Step 2. Level the cabinet 8
Step 3. Attach the stabilizers 9
Step 4. Attach the cabinet to a concrete floor 10
Step 5. Attach the cabinet to a concrete floor beneath a raised floor 12
Step 6. Attach the mounting plates 15
Step 7. Attach the front door 16
Step 8. Check the customer's ac power source 16
Step 9. Check the power distribution unit 17
External ac power cords 17
Step 10. Connect switch and device cables 18
Step 11. Power on the cabinet 18

Chapter 3. Starting and configuring the 2109 Model M12 19
Providing initial power to the chassis 19
Configuring the 2109 Model M12 19
Items needed 20
Configuration procedure 21

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1270
3690
Doc:

Chapter 4. Operating the 2109 Model M12 27
Turning on and off the 2109 Model M12. 27
Switch components 27
16-port cards 28
Control processor cards 28
Power supplies 30
ac power input connectors and ac power switches (circuit breaker). 30
Blower assemblies 30
WWN card and bezel 31
Cable management items 31
Interpreting LED activity 32
LEDs on the 16-port card 32
LEDs on the CP card 35
LEDs on the power supply 38
LEDs on the blower assembly 40
LEDs on the WWN card and bezel 41
Interpreting POST. 42
Maintaining the switch 43
Diagnostic tests 43
Field replaceable units 43
Environmental status and maintenance commands 44

Chapter 5. Installing modems 45
Setting up a remote modem system (optional) 46
Installing the modems on the 2109 Model M12 47
Verifying modem installation 48

Chapter 6. Installing and removing an additional 2109 Model M12 51
Installation considerations and safety guidelines. 51
Ordering the lift tool 52
2109 Model M12 standard shipment 53
Unpacking the 2109 Model M12 53
Installing the 2109 Model M12 in the cabinet 55
Time required 55
Tools required 55
Installing the brackets 55
Using the lift tool, the 24-inch load plate, and the bridge tool 60
Removing a 2109 Model M12 from the cabinet 65

Chapter 7. Servicing the 2109 Model C36 with Model M12 69
Safety notices 69
Power-on procedure 69
Power-off procedure 70
Removing and replacing a 16-port card or filler panel. 70
Time required 70
Removing a 16-port card or filler panel 70
Replacing a 16-port card or filler panel 74
Guidelines for managing cables. 75
Removing and replacing a CP card or filler panel 75
Time required 76
Items required 76
Confirming a failed CP card 76
Recording critical switch information for a CP card 77
Removing a CP card or filler panel 79
Replacing a CP card or filler panel 81
Verifying the operation of the new CP card 82

Replacing the CP card battery 86
Removing and replacing a power supply or filler panel 86
Time required 87
Removing a power supply or filler panel. 87
Replacing a power supply or filler panel. 89
Removing and replacing a blower assembly 89
Time required 90
Items required 90
Removing a blower assembly 90
Replacing a blower assembly 90
Removing and replacing the cable management tray 91
Time required 91
Items required 91
Removing a cable management tray 91
Replacing a cable management tray 92
Removing and replacing the WWN card. 93
Verifying if the WWN needs replacing 93
Data that is stored on the WWN card 94
Messages that might indicate WWN card failure. 94
Removing and replacing the PDU 94
Removing the PDU 95
Replacing the PDU 95
Removing and replacing the chassis door 95
Time required 95
Removing the chassis door 96
Replacing the chassis door 96
Removing and replacing the front or rear cabinet door 96
Removing the cabinet door 96
Replacing the cabinet door 97
Relocating the cabinet 97
Reference information for the fruinfoset command 97

Appendix A. Product specifications 99
2109 Model M12 components 99
Physical dimensions 99
2109 Model M12 and component weights 99
2109 Model C36 with Model M12 specifications 100
16-port card specifications 100
CP card specifications. 101
Fibre Channel port specifications. 102
Facility specifications 103
Power specifications 103
Environmental requirements 104
General specifications. 105
Regulatory specifications. 106
POST and Boot specifications. 107
Monitoring POST results 107
Boot 108

Appendix B. Parts information 109
Covers 109
Earthquake brace 110
Blank fillers 111
Stabilizers 112
Leveling feet 113
Power cords 113

RQS nº 03/2005 - CN -
CPMI. - CORREIOS
Fls. Nº 1271
Doc: 3690

Cabinet parts list 115
Power distribution unit (PDU) 116
2109 Model M12 parts list 117

Appendix C. Blank planning worksheets 119
Planning worksheet 119
Port configuration worksheet 120
Zone definition worksheet 121
Zone configuration worksheet 122

Notices 123
Trademarks. 124
Electronic emission statements 124
Federal Communications Commission (FCC) statement 124
Industry Canada compliance statement 124
Chinese Class A compliance statement 124
European Community compliance statement 125
Germany compliance statement 125
Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 126
Korean Government Ministry of Communication (MOC) statement 126
Taiwan class A compliance statement 126

Glossary 127

Index 141

Figures

1. Agency Certification label on the 2109 Model C36 . . . xii
2. Power supply cord caution label on the 2109 Model C36 . . . xii
3. High leakage current danger label on the 2109 Model C36 . . . xiii
4. Safety label on the 2109 Model M12 . . . xv
5. Linecord caution label . . . xv
6. Power supply cover caution label . . . xvi
7. Fusing caution label . . . xvi
8. Heavy load label . . . xvi
9. SFP label (front view) . . . xvii
10. SFP label (back view) . . . xvii
11. Bridge tool alignment label . . . xix
12. Tilt warning label . . . xx
13. Genie tool and load plate label . . . xx
14. Pinch point label . . . xxi
15. Port side of the 2109 Model M12 . . . 3
16. Blower assembly side of the 2109 Model M12 . . . 4
17. Caster wheel . . . 8
18. Adjusting the leveling feet . . . 9
19. Stabilizers . . . 9
20. Attaching the cabinet to a concrete floor . . . 10
21. Leveling the cabinet . . . 12
22. Attaching the cabinet to a raised floor . . . 13
23. Leveling the cabinet . . . 14
24. Attaching the mounting plate . . . 15
25. Attaching the front door . . . 16
26. 16-port card LEDs . . . 33
27. CP card LEDs . . . 36
28. Power supply LEDs . . . 38
29. Blower assembly LEDs . . . 40
30. LEDs on the WWN card and bezel . . . 42
31. 2109 Model M12 with two modems connected . . . 46
32. 2109 Model M12 on a pallet . . . 54
33. Removing the chassis door . . . 55
34. Placement of the shelf brackets and clip nuts on the cabinet rails . . . 56
35. Shelf brackets are installed on the rails (cabinet walls are not shown) . . . 57
36. Placing the clip nuts on the rear rails (service aisle side) . . . 58
37. Attaching the right and left flat upper mount brackets to the chassis . . . 59
38. Attaching the L-shaped upper mount brackets to the rails . . . 59
39. Rear view of cabinet and lift tool . . . 61
40. Locking the shelf into position . . . 62
41. Attaching the mount brackets to the cabinet rails . . . 63
42. Attaching the port side of the chassis to the cabinet rails . . . 64
43. Removing the chassis door . . . 65
44. 16-port card showing ejectors . . . 72
45. 16-port card filler panel . . . 73
46. CP card filler panel with one handle . . . 74
47. Alignment guides in the card slots . . . 75
48. CP card showing ejectors . . . 80
49. CP card filler panel with two ejectors . . . 81
50. Alignment guides in the card slots . . . 82
51. Location of the power supplies . . . 88
52. Power supply and filler panel . . . 89
53. Blower assembly side of the 2109 Model M12 shown with one blower assembly uninstalled . . . 91

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1272
3690
Doc:

54. Cable management tray 92
55. 2109 Model M12 with the cable management tray 93
56. Removing the cabinet door 96
57. Front view of the PDU 116
58. Top view of the PDU 117

Tables

1. Brocade and IBM product and model number matrix xxiv
2. Configuration parameters 21
3. 16-port card LED patterns 33
4. CP card LED patterns 37
5. Power supply LED patterns 39
6. Blower assembly LED patterns 40
7. Modem parameters for Windows 95, 98, 2000, ME, or NT, or TERM in a UNIX environment 47
8. Parameters and values 77
9. Data that the WWN card stores 94
10. Sample error messages 94
11. Reference information for the fruinfoset command 97
12. Physical dimensions of the 2109 Model M12 99
13. Component weights 99
14. 2109 Model C36 with Model M12 specifications 100
15. Memory specifications 101
16. Battery specifications 101
17. Pinouts with signal and description 102
18. Modem serial port pinouts 102
19. Power specifications 104
20. Environmental requirements 104
21. General specifications 105
22. Regulatory specifications 106
23. Items supplied with the 14U chassis mount kit 115
24. Planning worksheet 119
25. Port configuration worksheet 120
26. Zone definition worksheet 121
27. Zone configuration worksheet 122

RQS nº 03/2005 - CN -
CPMI -- CORREIOS
Fls. Nº 1273
Doc: 3690

© Copyright IBM Corp. 2002, 2003

Safety and environmental notices

This section contains information about:

- Safety notices that are used in this document
- Safety inspection procedures for this product
- Environmental guidelines for this product

Safety notices

This document contains the following safety notices:

A *Danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

A *Caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

An *Attention* notice indicates the possibility of damage to a program, device, system, or data.

Safety inspection procedures

This safety inspection procedure contains three parts:

- Inspecting the 2109 Model C36 cabinet
- Inspecting the 2109 Model M12 switch
- Inspecting the bridge tool, where applicable

This document uses the following terms:

- *Rack* refers to the metal framework of this unit.
- *Cabinet* refers to the rack, all the peripherals that are attached to the rack, and the 2109 Model M12 switch.

Inspecting the cabinet

Perform a safety inspection on the cabinet when any of the following conditions occur:

- The cabinet is inspected under a maintenance agreement.
- Service is requested and service has not recently been performed.
- An alteration-and-attachments review is performed.
- Changes were made to the equipment that might affect the safe operation of the equipment.
- External devices with an attached power cord are connected to the cabinet.

Be cautious of potential safety hazards that are not covered in the safety checks. If the inspection indicates an unacceptable safety condition, the condition must be corrected before you can service the machine.

Note: The owner of the system is responsible for correcting any unsafe condition.

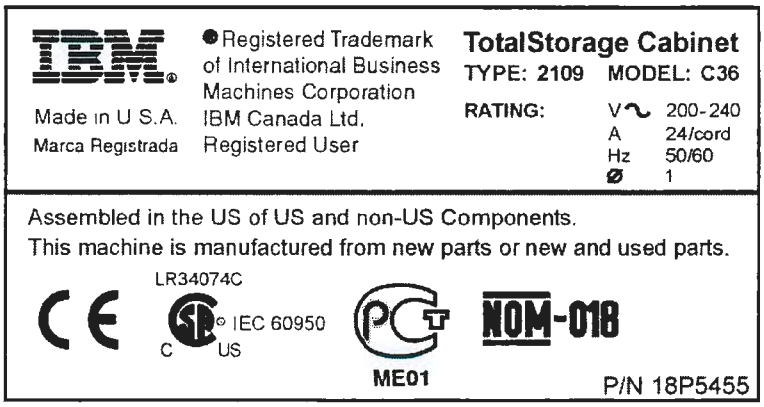
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1274
3690
Doc:

© Copyright IBM Corp. 2002, 2003

Cabinet safety label checks

Perform the following cabinet safety label checks:

1. Verify that the Agency Certification label shown in Figure 1 is installed on the 2109 Model C36.

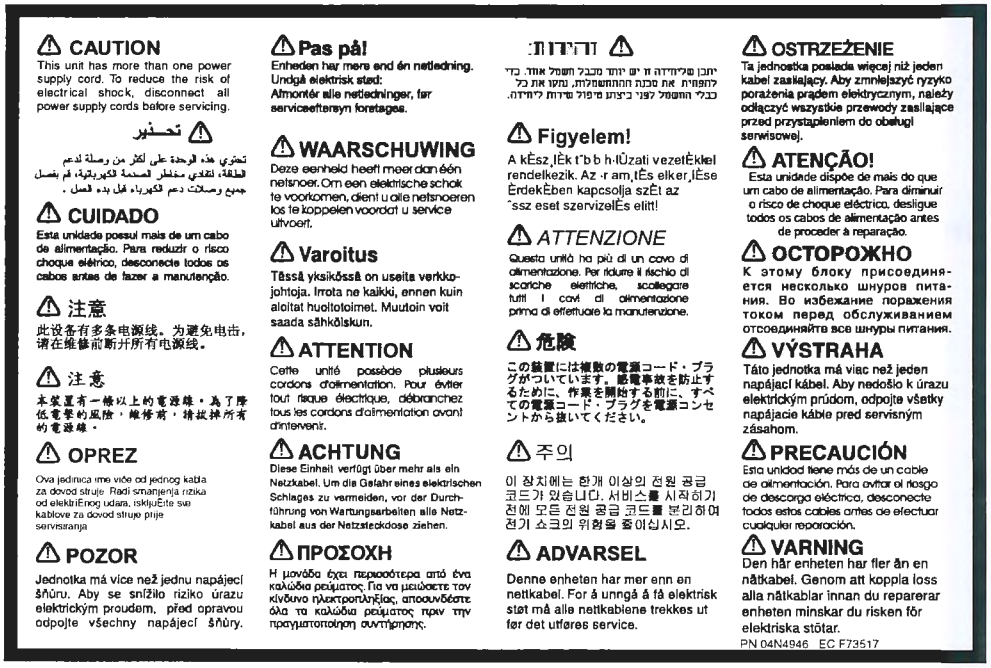


SJ000649

Figure 1. Agency Certification label on the 2109 Model C36

2. Verify that the power supply cord caution label shown in Figure 2 is installed on the 2109 Model C36.

   CAUTION:
   This unit has more than one power supply cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing.



SJ000650

Figure 2. Power supply cord caution label on the 2109 Model C36

3. Verify that the high leakage danger label shown in Figure 3 on page xiii is installed on the 2109 Model C36.

DANGER

HIGH LEAKAGE CURRENT. Earth connection essential before connection supply.

Figure 3. High leakage current danger label on the 2109 Model C36

External cabinet checks

Perform the following safety checks:

1. If the cabinet is bolted down, ensure that the cabinet is firmly secured to the floor. See Figure 20 on page 10.
2. If the cabinet is not bolted down, ensure that the stabilizers are firmly attached to both the bottom front and bottom rear of the rack. See Figure 19 on page 9.

   CAUTION:
   You must firmly attach the stabilizer to the bottom front and bottom rear of the cabinet to prevent the cabinet from turning over when the switches are pulled out of the cabinet.
3. Check the covers for sharp edges and for damage or alterations that expose the internal parts of the cabinet.
4. Check the covers for a proper fit to the cabinet. The covers should be in place and secure.
5. Open the rear door of the cabinet.
6. **CAUTION:**
   This unit might have more than one power supply cord. To completely remove power, you must disconnect all power supply cords.

   Perform the power-off procedure for the power distribution unit (PDU) that is installed in the cabinet. See "Power-off procedure" on page 70 for power-off procedures.
7. Check for alterations or attachments and obvious safety hazards such as broken wires, sharp edges, or broken insulation.

RQS nº 03/2005 - CN - CORREIOS
Fls. Nº 1275
3690
Doc:

8. Check the internal cables for damage.
9. Check for dirt, water, and any other contamination within the cabinet.
10. Check the voltage label on the back of the system unit to ensure that it matches the voltage at the outlet.
11. Check the external power cable for damage.
12. Perform the following grounding checks:
    a. With the external power cord connected to the system unit, check for 0.1 ohm or less resistance between the ground lug on the external power cord plug and the rack.
    b. Using the appropriate probe, check for 0.1 ohm or less resistance between the rack and the grounding pin on each of the power outlets on each power distribution bus.
13. Check for the following conditions for each external device that has an attached power cord:
    - Damage to the power cord.
    - The correct grounded power cord.
    - With the external power cord connected to the device, check for 0.1 ohm or less resistance between the ground lug on the external power cord plug and the rack of the cabinet.
14. Close the rear door of the cabinet.
15. Perform the power-on procedure for the PDU that is installed in the cabinet. See "Power-on procedure" on page 69.

Inspecting the 2109 Model M12

Perform the following safety checks to identify unsafe conditions.

Removing ac power

Perform the following steps to remove the alternating current (ac) power:

1. Perform a controlled system shutdown.
2. Set the power switches on the 2109 Model M12 to the off position.
3. Disconnect the power cord from the power source.

External machine checks

Perform the following external machine checks:

1. Verify that all external covers are present and are not damaged.
2. Ensure that all latches and hinges are in correct operating condition.
3. Check the power cord for damage.
4. Check the external signal cable for damage.
5. Check the cover for sharp edges, damage, or alterations that expose the internal parts of the device.
6. Correct any problems that you find.

Internal machine checks

Perform the following internal machine checks:

1. Check for any non-IBM changes that might have been made to the machine. If any are present, obtain the "Non-IBM Alteration Attachment Survey" form, number R009, from the IBM branch office. Complete the form and return it to the branch office.
2. Check the condition of the inside of the machine for:
    - Metal or other contaminants

- Indications of water or other fluid
- Fire
- Smoke damage

3. Check for any obvious mechanical problems, such as loose components.
4. Check any exposed cables and connectors for wear, cracks, or pinching.

Safety label checks

Perform the following safety label checks:

1. Verify that the safety label shown in Figure 4 is installed on the 2109 Model M12.

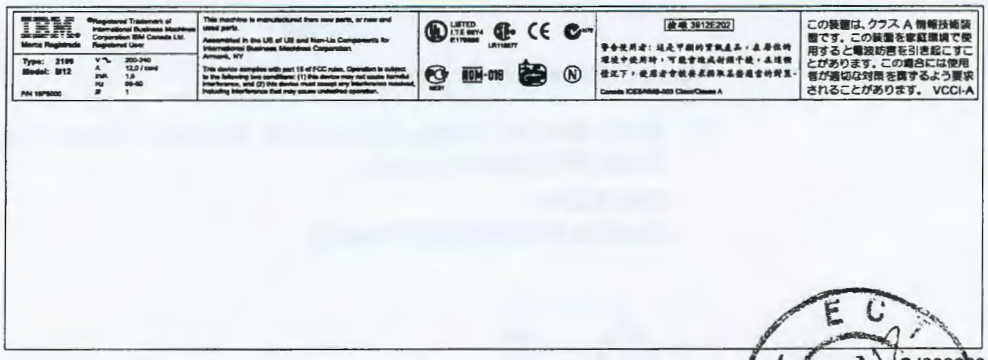


Figure 4. Safety label on the 2109 Model M12

2. Verify that the linecord caution label shown in Figure 5 is installed on the 2109 Model M12 power supply.

   CAUTION:
   This unit might have two linecords. To remove all power, disconnect both linecords.

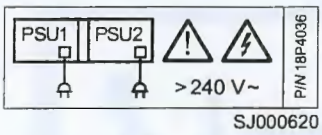
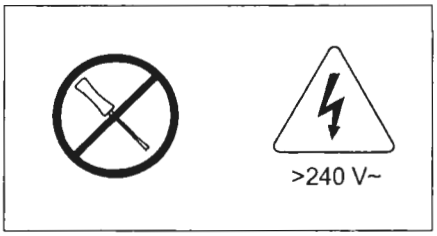


Figure 5. Linecord caution label

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1276
Doc: 3690

3. Verify that the power supply cover caution label shown in Figure 6 is installed on the 2109 Model M12 power supply.

   CAUTION:
   Do not remove cover, do not service, no serviceable parts.

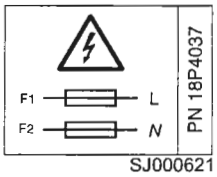


SJ000323

Figure 6. Power supply cover caution label

4. Verify that the fusing caution label shown in Figure 7 is installed on the 2109 Model M12 power supply.

   CAUTION:
   Double Pole/Neutral Fusing.



SJ000621

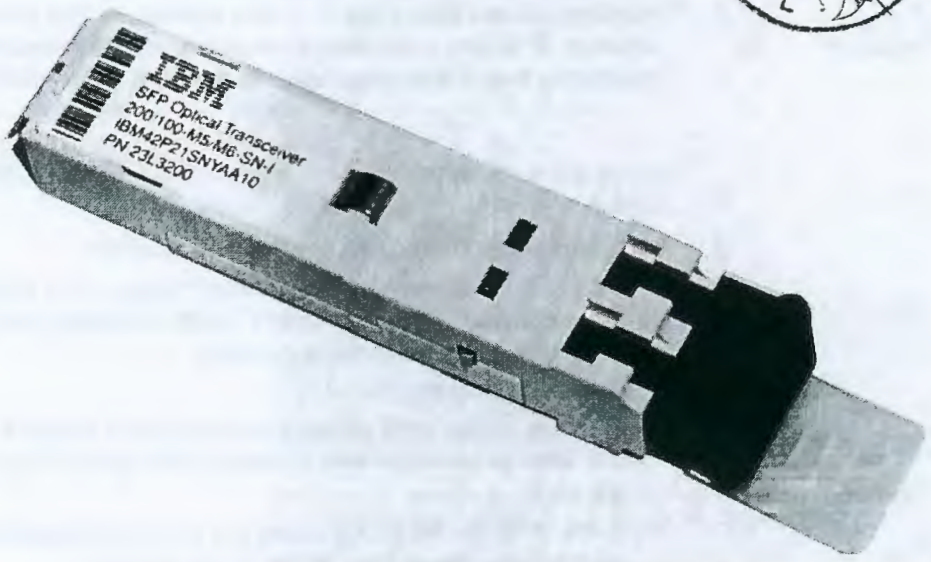
Figure 7. Fusing caution label

5. Verify that the heavy load label shown in Figure 8 is installed on the back of the 2109 Model M12.

SJ000625

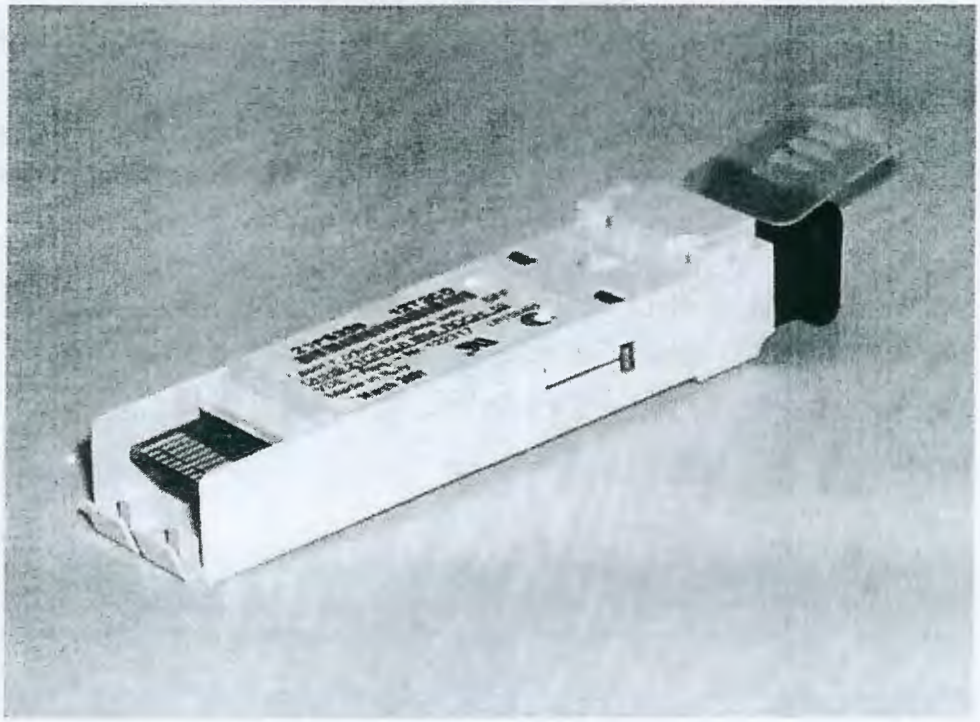
Figure 8. Heavy load label

6. Verify that the SFP label shown in Figure 9 and Figure 10 is installed on the 2109 Model M12.



SJ000317

Figure 9. SFP label (front view)



SJ000314

Figure 10. SFP label (back view)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1277
Doc: 3690

Checking ac grounding

DANGER

An electrical outlet that is not correctly wired could place a hazardous voltage on the metal parts of the system or the products that attach to the system. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (1)

Check the voltage label on the bottom of the device to ensure that it matches the voltage at the power source.

1. Check the voltage level at the power source.
2. **Attention:** Always use an analog meter, never a digital meter, to perform the ground check of the customer's outlet. A digital meter can give the wrong reading if ground current is present.

   Check for proper grounding.
3. With the power cord connected to the 2109 Model M12, verify that there is 0.1 ohm or less resistance between the ground lug on the power cord plug and the rack.
4. If the 2109 Model M12 passes the ac grounding check (step 1 - step 3), connect the power cord to the power source.

Inspecting the bridge tool

Note: The bridge tool (PN 18P5855) is only shipped with a replacement 2109 Model M12 and is not part of the normal ship group. Inspect the bridge tool and ensure that the two adjustable supports are securely fastened and are rotated 90° from the base plate.

Perform the following safety label checks for the bridge tool:

1. Verify that the bridge tool alignment label shown in Figure 11 on page xix is installed on the load plate.

Figure 11. Bridge tool alignment label

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1278
3690
Doc:

2. Verify that the tilt warning label shown in Figure 12 is installed on the load plate.

SJ000750

Figure 12. Tilt warning label

3. Verify that the genie tool and load plate label shown in Figure 13 is installed on the load plate.

SJ000751

Figure 13. Genie tool and load plate label

4. Verify that the pinch point label shown in Figure 14 is installed on the load plate.

SJ000752

Figure 14. Pinch point label

Environmental notices and statements

This section describes the environmental notices and statements.

Laser safety

CAUTION:
In the United States use only GBIC units or Fibre-Optic products that comply with FDA radiation performance standards, 21 CFR Subchapter J. Internationally use only GBIC units or Fibre-Optic products that comply with IEC standard 825-1. Optical products that do not comply with these standards may produce light that is hazardous to the eyes.

SJ000327

This unit might contain a single-mode or a multimode transceiver Class 1 laser product. The transceiver complies with IEC 825-1 and FDA 21 CFR 1040.10 and 1040.11. The transceiver must be operated under the recommended operating conditions.

This equipment contains Class 1 laser products and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser-safety standard IEC 825-2.

Usage restrictions

Terminate the optical ports of the modules with an optical connector or a dust plug.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1570
3690
Doc:

Battery notice

CAUTION:
A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery might present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations.

Fire suppression systems

A fire suppression system is the responsibility of the customer. The customer's own insurance underwriter, local fire marshal, or a local building inspector, or both, should be consulted in selecting a fire suppression system that provides the correct level of coverage and protection. IBM designs and manufactures equipment to internal and external standards that require certain environments for reliable operation. Because IBM does not test any equipment for compatibility with fire suppression systems, IBM does not make compatibility claims of any kind nor does IBM provide recommendations on fire suppression systems.

See "Environmental requirements" on page 104.

Product recycling

This unit contains recyclable materials. Recycle these materials where processing sites are available and according to local regulations. In some areas, IBM provides a product take-back program that ensures proper handling of the product. Contact your IBM representative for more information.

Product disposal

This unit might contain batteries. Remove and discard these batteries, or recycle them, according to local regulations.

About this document

This document provides installation and maintenance information for the IBM® TotalStorage™ SAN Cabinet 2109 Model C36 with Model M12 switch.

This document uses the following terms:

- *Rack* refers to the metal framework of this unit.
- *Cabinet* refers to the rack, all the peripherals that are attached to the rack, and the 2109 Model M12 switch.

Who should read this document

This document is intended for the service support representative to install or repair the 2109 Model C36 with Model M12 switch.

Additional information

This section contains the following information:

- A list of the documents in the 2109 Model C36 with Model M12 library
- A list of the related documents
- The available Web sites
- Instructions on how to get help
- Instructions on how to get software updates
- Information about how to send your comments

2109 Model C36 with Model M12 library

The following documents contain information related to this product:

- *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*, GC26-7467 (this book)
- *IBM TotalStorage SAN Switch 2109 Model M12 User's Guide*, GC26-7468

Related documents

You can find Information related to the software that supports the 2109 Model M12 in the following documents:

- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Diagnostic and System Error Message Reference*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Reference*
- *Brocade Fabric Watch User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade MIB Reference*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Silkworm 12000 Core Migration User's Guide*

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1280
Doc: 3690

For utility programs to facilitate loading firmware, sample Fabric Watch configurations, and management information base (MIB) files for switch management by simple network management protocol (SNMP), see the following Web site:

www.storage.ibm.com/ibmsan/products/sanfabric.htm

How to send your comments

Your feedback is important to help us provide the highest quality of information. If you have any comments about this document, you can submit them in one of the following ways:

- E-mail

  Submit your comments electronically to:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the document and, if applicable, the specific location of the text that you are commenting on, such as a page number or table number.

- Mail or fax

  Fill out the Readers' Comments form (RCF) at the back of this document and return it by mail or fax (1-800-426-6209) or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Dept. M86/Bldg. 050-3
  5600 Cottle Road
  San Jose, CA 95193-0001
  U.S.A.

DPMT = CORNEIUS
1281
3690

Chapter 1. Introduction

This chapter introduces the 2109 Model M12 switch (hereafter referred to as the 2109 Model M12) and contains the following information:

- Overview of the 2109 Model M12
- How to monitor and manage the 2109 Model M12

The IBM factory installs the 2109 Model M12 and ships it in the 2109 Model C36 cabinet.

Overview

The 2109 Model M12 is a high-performance core switch for large storage area networks (SANs), available in 16-port increments from 32 - 128 ports. It can operate as a single switch in a fabric or in a fabric that contains multiple switches.

High-availability features of the 2109 Model M12 include:

- Two redundant hot-swappable control processor (CP) cards with automatic failover
- Up to eight hot-swappable 16-port cards
- Four hot-swappable power supplies
- Three hot-swappable blower assemblies (two are required for adequate cooling)
- Two redundant ac inputs
- Non-disruptive upgrades for Fabric OS v4.1
- Worldwide name (WWN) card that is hot-swappable in Fabric OS v4.1

The 2109 Model M12 also includes the optional Advanced Security feature, which enables policy-based security mechanisms integrated with certain versions of the Fabric OS. The optional Advanced Security feature has the following capabilities:

- Centralized security management
- Fabric-wide security policies to control access
- Port and switch level access control
- Management access controls (Telnet, SNMP, HTTP, API)
- Encryption of management data such as passwords
- Strong and non-reputable authentication between switches

The Fibre Channel ports support link speeds of 1 Gbps and 2 Gbps (inbound and outbound). They also automatically negotiate to the highest common speed of all the devices that are connected to the port and are:

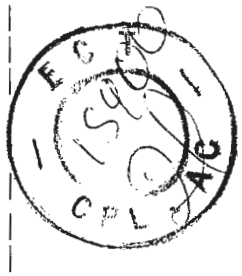
- Compatible with short wavelength (SWL) and long wavelength (LWL) small form factor pluggable (SFP) transceivers
- Universal and self-configuring
- Capable of individually becoming fabric loop ports (FL_ports), fabric ports (F_ports), or expansion ports (E_ports)

For the 2109 Model M12 specifications, see Appendix A, "Product specifications", on page 99.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1282
Doc: 3690

© Copyright IBM Corp. 2002, 2003

Software features



Fabric OS version 4.1 supports the 2109 Model M12. Fabric OS includes all the basic switch and fabric support software as well as optionally licensed software that is enabled by using license keys. Fabric OS is made up of two major software components: firmware that initializes and manages the switch hardware, and diagnostics.

Optionally licensed and separately priced features include:

- Extended Fabrics (Feature code 7603)

  Provides up to 100 km (62.14 mi) of switched fabric connectivity at full bandwidth over long distances
- Remote Switch (Feature code 7602)

  Enables switches to interconnect over wide area network (WAN) using third-party gateway solutions that support Fibre Channel (FC) over Internet Protocol (IP), FC over asychronous transfer mode (ATM), and FC over SONET
- Advanced Security (Feature code 7623)

  Enables policy-based security mechanisms that are integrated within Fabric OS

Note: To activate these features, go to the following Web site:

www.ibm.com/storage/key/

The following licensed software provides a graphical user interface from a standard workstation:

- Fabric Manager 4.0 (Feature code 7203)

  Administers, configures, and maintains fabric switches and SANs with host-based software

The following licensed products are included with the 2109 Model M12:

- Performance Monitoring

  Comprehensive tool for monitoring the performance of network storage resources
- ISL Trunking

  Connects up to four ISLs between two switches through an expansion port (E_port) to merge logically into one link
- Fabric Watch

  Monitors mission-critical fabric parameters
- Advanced Zoning

  Segments a fabric into virtual private SANs
- Web Tools

  Administers, configures, and maintains fabric switches and SANs

See the following documents for more information about Fabric Watch, Fabric Manager, Web Tools, Secure Fabric OS, and high availability:

- *Brocade Advanced Zoning User's Guide*
- *Brocade Fabric Watch User's Guide*
- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Distributed Fabrics User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Advanced Web Tools User's Guide*

Port side of chassis

Figure 15 shows the port side of the 2109 Model M12, which provides access to the following components:

- The 16-port cards, which contains 16 Fibre Channel SFP ports
- Two CP cards, each with a modem serial port, a terminal serial port, and 10 Mbps or 100 Mbps Ethernet port
- Four power supplies that are hot-swappable and have built-in fans
- Two ac power connectors. Each ac power connector has an on or off ac power switch

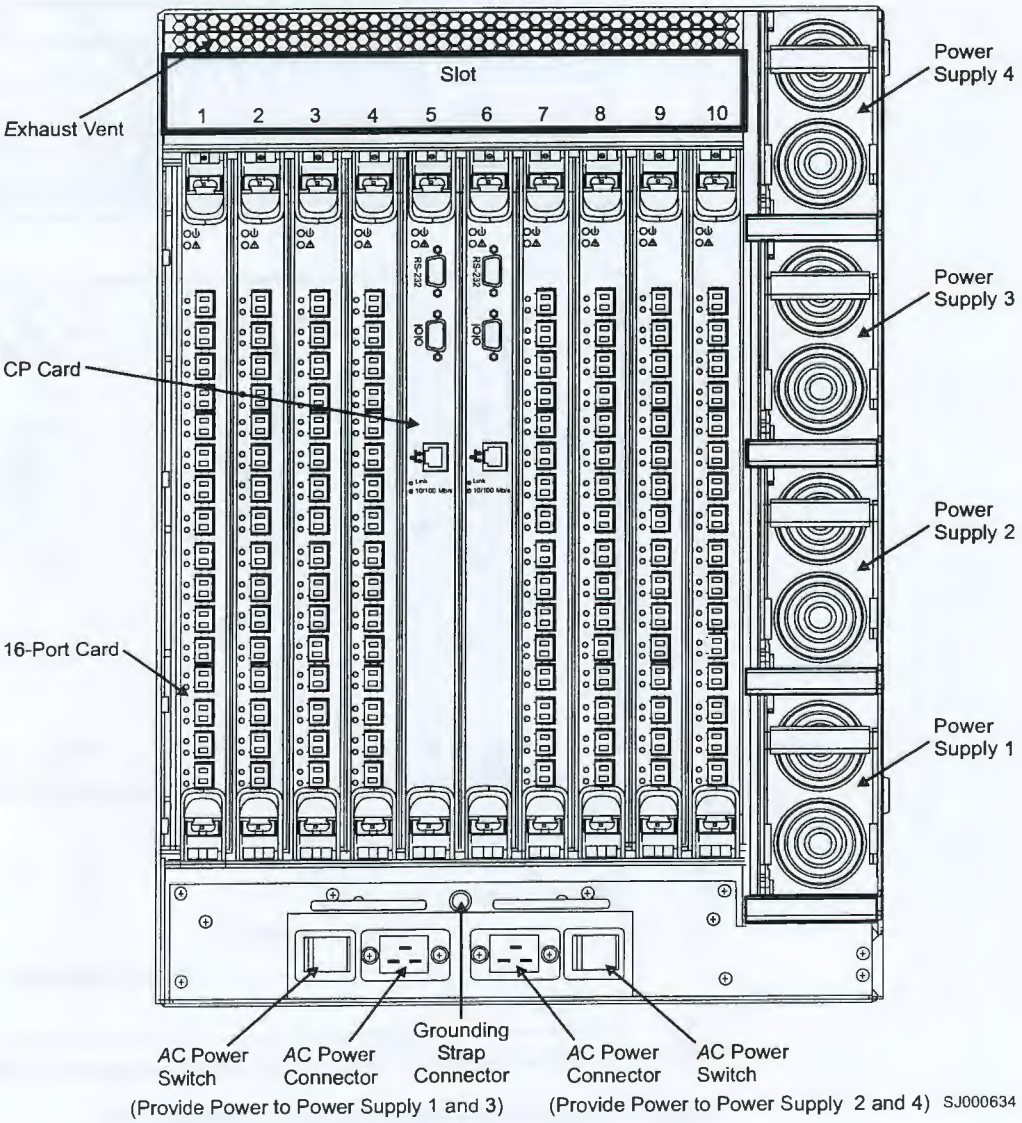


Figure 15. Port side of the 2109 Model M12

For information about how to operate the components of the 2109 Model M12, see Chapter 4, "Operating the 2109 Model M12", on page 27.

ROG nº 09/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1283
Doc: 3690

Blower assembly side of chassis

Figure 16 shows the blower assembly side of the 2109 Model M12, which provides access to the following components:

- A WWN card and bezel. The WWN card and bezel provide light-emitting diodes (LEDs) for monitoring the switch from the blower assembly side and store WWN and IP address information, switch name, and serial number.
- Three blower assemblies. Each blower assembly is individually hot-swappable.

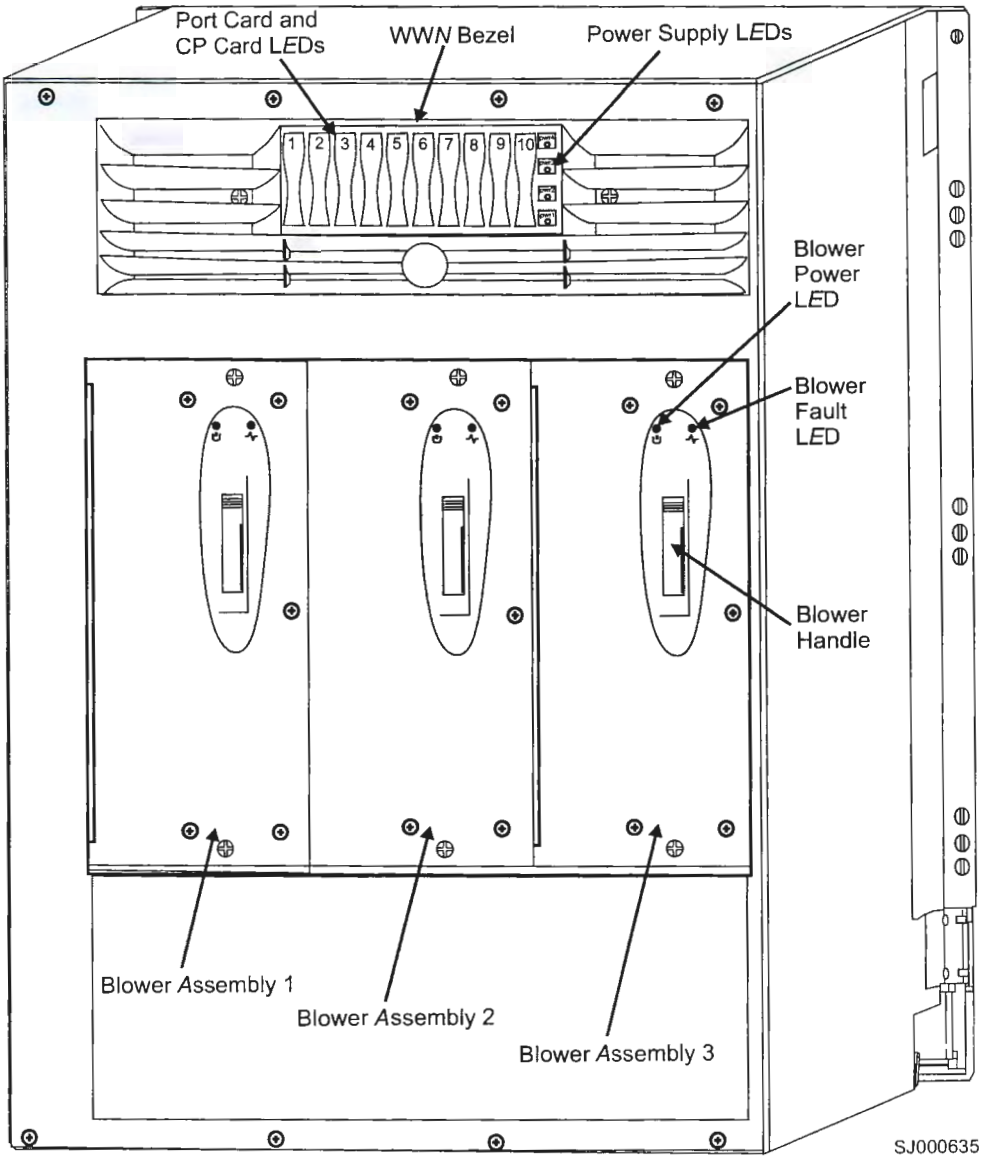


Figure 16. Blower assembly side of the 2109 Model M12

Monitoring and managing the 2109 Model M12

You can manage the 2109 Model M12 in-band by using Fibre Channel protocol or out-of-band by connecting to the Ethernet port. The management functions allow the administrator to monitor fabric topology, port status, physical status, and other information to aid in performance analysis and system debugging.

Note: The 2109 Model M12 automatically performs power-on self-test (POST) diagnostics each time it is turned on. Any errors are recorded in the error log. For more information about POST, see "Interpreting POST" on page 42.

The 2109 Model M12 is compatible with the following management interfaces:

- Command line interface through a Telnet connection
- Fabric Manager
- Web Tools
- SNMP applications
- Management server

You can manage these methods either in-band (Fibre Channel) or out-of-band (Ethernet).

For more information about these management interfaces, see the *Brocade Fabric Manager User's Guide* and the *Brocade Advanced Web Tools User's Guide*.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1284
3690
Doc:

Chapter 2. Installing the 2109 Model C36

This section contains the procedures to install a 2109 Model C36 (hereafter referred to as the *cabinet*) and prepare it for use.

The following safety notices apply to the procedures in this chapter. Review this section carefully before you install the cabinet.

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

Before you install or remove signal cables, ensure that the power cables for the system unit and all attached devices are unplugged.

When you add or remove any additional devices to or from the system, ensure that the power cables for those devices are unplugged before you connect the signal cables. If possible, disconnect all power cables from the existing system before you add a device.

Use one hand, when possible, to connect or disconnect signal cables to prevent a possible shock from touching two surfaces with different electrical potentials.

During an electrical storm, do not connect cables for display stations, printers, telephones, or station protectors for communication lines.

CAUTION:
This product is equipped with a 3-wire power cable and grounded plug for the user's safety. Use this power cable in conjunction with a properly grounded electrical outlet to avoid electrical shock.

CAUTION:
This unit might have more than one power supply cord. To completely remove power, you must disconnect all power supply cords.

Step 1. Position the cabinet

Note: IBM must install the IBM 2109 Model C36.

Perform the following steps to position the cabinet:

1. Remove all packing and tape from the cabinet.
2. Position the cabinet according to the customer floor plan.
3. Lock each caster wheel by tightening the screw on the caster. See Figure 17 on page 8.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
1285
Fls. Nº
3690
Doc:

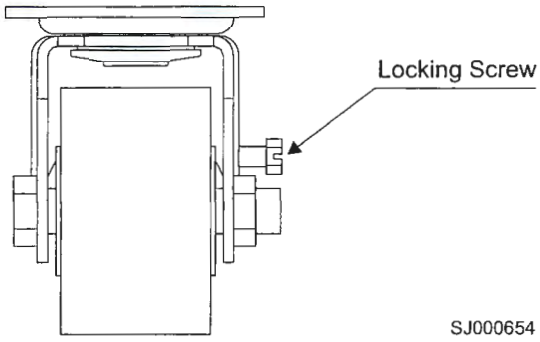


Figure 17. Caster wheel

Use the following conditions to determine the next step:

- If you are not attaching the cabinet to the floor, go to "Step 2. Level the cabinet".
- If you are bolting the cabinet to a concrete floor, go to "Step 4. Attach the cabinet to a concrete floor" on page 10.
- If you are bolting the cabinet to a concrete floor beneath a raised floor, go to "Step 5. Attach the cabinet to a concrete floor beneath a raised floor" on page 12.

Step 2. Level the cabinet

Perform the following steps to adjust the leveling feet:

1. Loosen the jam nut on each leveling foot by turning the nut counterclockwise, away from the bottom of the cabinet. See Figure 18 on page 9.
2. Rotate each leveling foot downward until it contacts the surface on which the cabinet is placed.
3. Adjust the leveling feet downward as needed until the cabinet is level. When the cabinet is level, tighten the jam nuts against the base by turning the nut clockwise, toward the bottom of the cabinet.

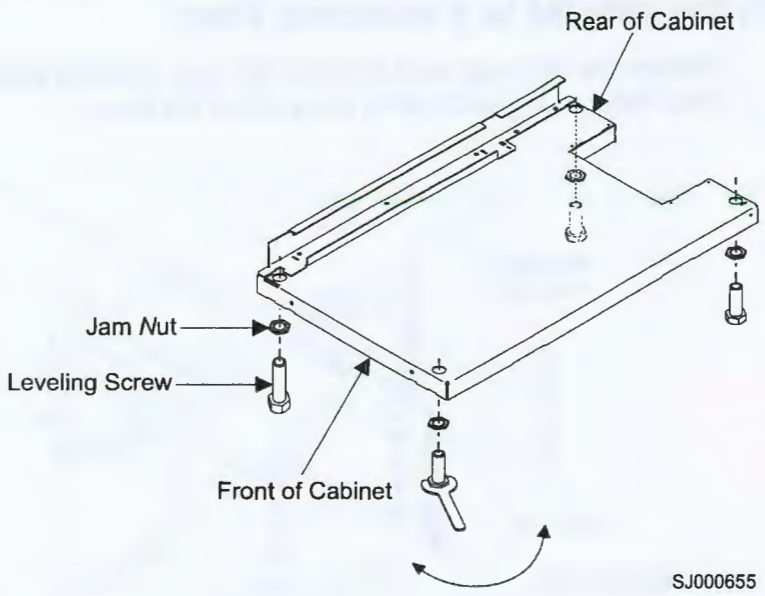


Figure 18. Adjusting the leveling feet

Step 3. Attach the stabilizers

CAUTION:
You must firmly attach the stabilizers to the bottom front and bottom rear of the cabinet to prevent the cabinet from turning over when the switches are pulled out of the cabinet.

1. Align the slots in the stabilizer with the mounting holes at the bottom front of the cabinet. See Figure 19.

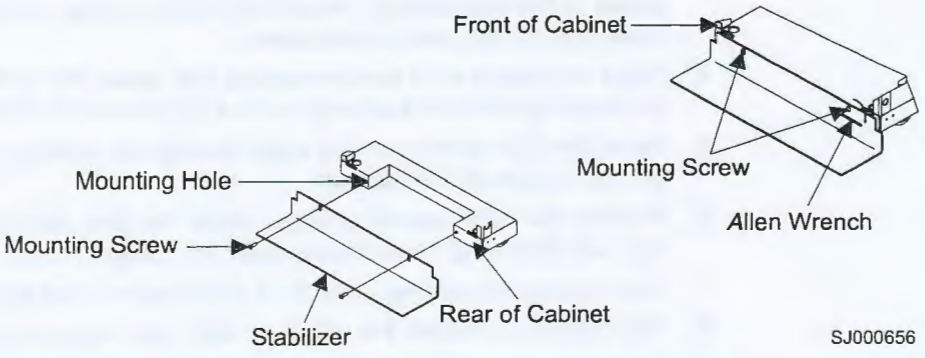


Figure 19. Stabilizers

2. Install the two mounting screws.
3. Ensure that the base of the stabilizer rests firmly on the floor. Use the allen wrench that is supplied with the cabinet to alternately tighten the mounting screws until they are tight.
4. Repeat step 1 through step 3 to install the stabilizer at the bottom rear of the cabinet.

CPMI - CORREIOS
1286
Fls. N°
Doc. 3690

Step 4. Attach the cabinet to a concrete floor

Perform the following steps to attach the rack-mounting plates directly to a concrete floor. Refer to Figure 20 while you perform the steps.

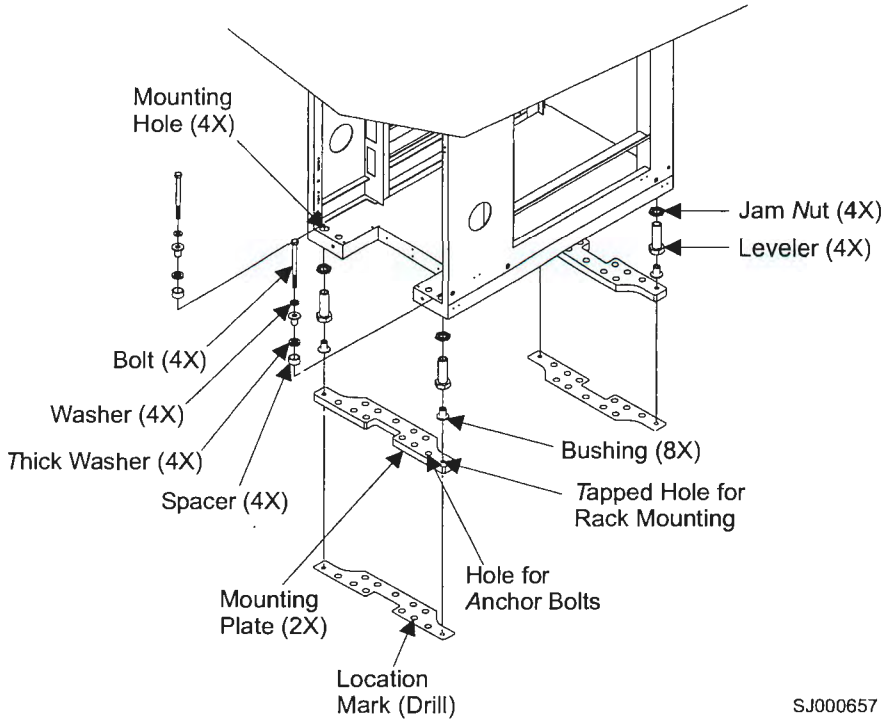


Figure 20. Attaching the cabinet to a concrete floor

1. Ensure that the cabinet is in the correct location.
2. In this cabinet, temporarily install the bushings to help position the rack-mounting plates.
3. Ensure that the bushing is in the leveling foot. Position the two rack-mounting plates in the approximate mounting location under the cabinet. If necessary, raise the leveling feet for clearance.
4. Place a bushing on a rack-mounting bolt. Insert the bolt and bushing through the leveling foot and bushing and out the bottom bushing.
5. Insert the four rack-mounting bolts through the leveling feet and bushings and out the bottom of the cabinet.
6. Position the rack-mounting plates under the four rack-mounting bolts. Center the rack-mounting bolts directly over the tapped holes.
7. Turn the rack-mounting bolts 3 - 4 rotations into the tapped holes.
8. Mark the floor around the edges of both rack-mounting plates.
9. Mark the rack-mounting plate bolt-down holes that are accessible through the opening in the rear of the cabinet.
10. Remove the rack-mounting bolts and bushings.
11. Remove the rack-mounting plates.
12. Loosen the locking screws on the casters. Move the cabinet so that the cabinet is clear of the locator marks for the rack-mounting plates.
13. Position the rack-mounting plates within the marked areas.

14. Mark the floor at the center of each hole in the rack-mounting plates (including the tapped holes).
15. Remove the two rack-mounting plates from the marked locations.
16. At the marked location of the tapped rack-mounting bolt holes, drill four holes approximately 5 cm (2 in.). This allows clearance for the ends of the four rack-mounting bolts. The ends of the rack-mounting bolts protrude past the thickness of the mounting plate.

    Note: You must use a minimum of two anchor bolts for each rack-mounting plate to attach it to the concrete floor. Because some of the holes in the rack-mounting plates might align with the concrete reinforcement rods that are below the surface of the concrete, some of the rack-mounting plate holes might not be suitable.
17. For each rack-mounting plate, select at least two suitable holes. Select holes as close to the threaded holes as possible. Be sure that the holes you select at the rear of the cabinet are accessible. Drill the selected holes (two for each rack-mounting plate).
18. Position the front rack-mounting plate within the marked area.
19. Using anchor bolts, attach the front rack-mounting plate to the concrete floor.

    Note: Do not use the four plastic isolator bushings.
20. Position the cabinet over the front rack-mounting plate.
21. Position the rear rack-mounting plate within the marked area.
22. Using anchor bolts, attach the rear rack-mounting plate to the concrete floor.
23. Insert each of the rack-mounting bolts through a flat washer, a thick washer, and through a leveling foot.
24. Align the four rack-mounting bolts with the four tapped holes in the two rack-mounting plates and turn the bolts 3 - 4 rotations.
25. Tighten the locking screw on each caster.
26. Adjust the leveling screw downward, as needed, until the cabinet is level. See Figure 21 on page 12. When the cabinet is level, tighten the jam nuts against the base by turning the jam nut clockwise, toward the bottom of the cabinet. Torque the four bolts to 54 - 67 nm (40 - 50 ft-lbs).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1287
3690
Doc:

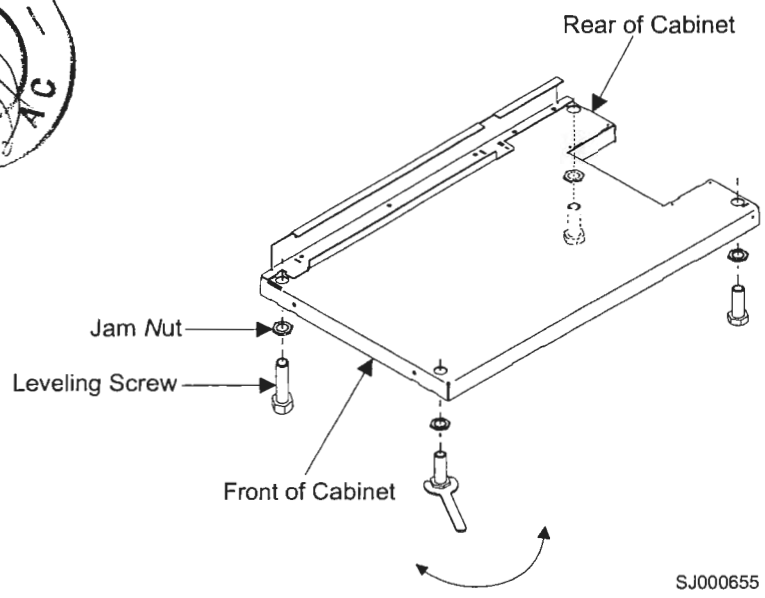


Figure 21. Leveling the cabinet

27. After you bolt down the cabinet, go to "Step 6. Attach the mounting plates" on page 15.

Step 5. Attach the cabinet to a concrete floor beneath a raised floor

Perform the following steps to attach the rack-mounting plates to the concrete floor beneath a raised floor.

Refer to Figure 22 on page 13 while you perform the steps.

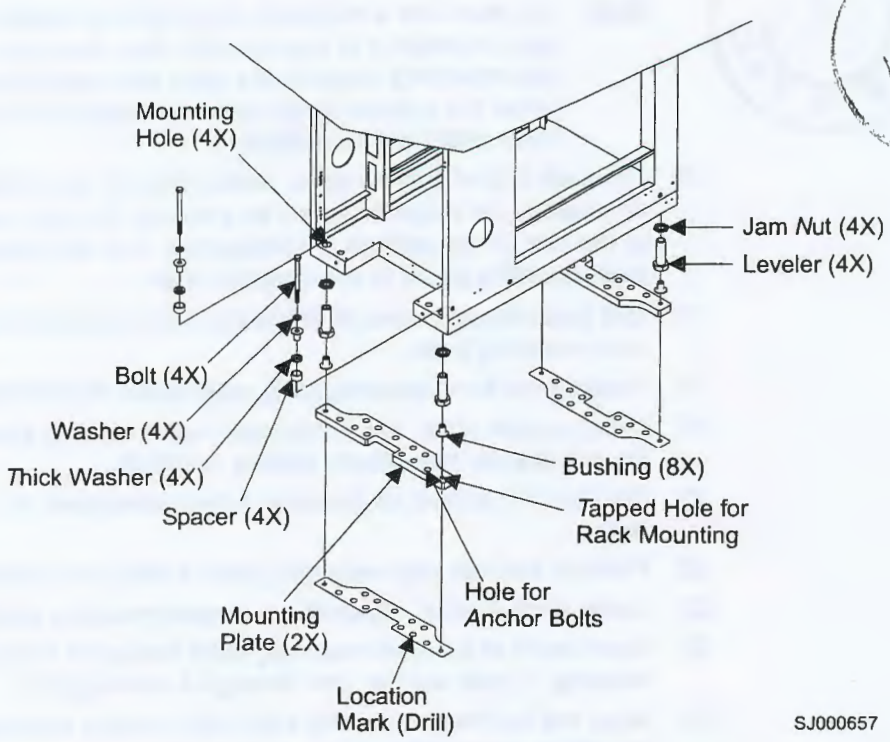


Figure 22. Attaching the cabinet to a raised floor

1. Ensure that the cabinet is in the correct location.
2. In this cabinet, temporarily install the bushings to help position the rack-mounting plates.
3. Ensure that the bushing is in the leveling foot. Position the two rack-mounting plates in the approximate mounting locations under the cabinet. If necessary, raise the leveling feet for clearance.
4. Place a bushing on a rack-mounting bolt. Insert the bolt and bushing through the leveling foot and bushing, and out of the bottom bushing.
5. Insert the four rack-mounting bolts through the leveling feet and bushings, and out the bottom of the cabinet.
6. Position the rack-mounting plates under the four rack-mounting bolts. Center the rack-mounting bolts directly over the tapped holes.
7. Turn the rack-mounting bolts 3 - 4 rotations into the tapped holes.
8. Mark the raised-floor panel around the edges of both rack-mounting plates.
9. Mark the rack-mounting plate bolt-down holes that are accessible through the opening in the rear of the cabinet.
10. Remove the rack-mounting bolts and bushings.
11. Remove the rack-mounting plates.
12. Loosen the locking screws on the casters. Move the cabinet so that it is clear of the locator marks for the rack-mounting plates.
13. Position the rack-mounting plates within the marked areas.
14. Mark the raised-floor panel at the center of each hole in the rack-mounting plates (including the tapped holes).
15. Remove the two rack-mounting plates from the marked locations.
16. Transfer the locations of the holes from the raised-floor panel to the concrete floor directly beneath. Mark the holes on the concrete floor.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1288
3690
Doc:

Note: You must use a minimum of two anchor bolts for each rack-mounting plate to attach it to the concrete floor. Because some of the holes in the rack-mounting plates might align with concrete reinforcement rods below the surface of the concrete, some of the rack-mounting plate holes might not be suitable.

17. For each rack-mounting plate, select at least two suitable holes. Select holes as close to the threaded holes as possible. Be sure that the holes you select at the rear of the cabinet are accessible. Drill the selected holes (two for each rack-mounting plate) in the concrete floor.
18. Drill pass-through holes in the raised-floor panel at the location of the four rack-mounting bolts.
19. Position the front rack-mounting plate within the marked area.
20. Using anchor bolts, attach the front rack-mounting plate to the concrete floor. Do not use the four plastic isolator bushings.
21. Position the cabinet on the raised-floor panel over the front rack-mounting plate.
22. Position the rear rack-mounting plate within the marked area.
23. Using anchor bolts, attach the rear rack-mounting plate to the concrete floor.
24. Insert each of the rack-mounting bolts through a flat washer, a plastic isolator bushing, a thick washer, and through a leveling foot.
25. Align the four rack-mounting bolts with the four tapped holes in the two mounting plates and turn the bolts 3 - 4 rotations.
26. Tighten the locking screw on each caster.
27. Adjust the leveling feet downward, as needed, until the cabinet is level. See Figure 23. When the cabinet is level, tighten the jam nuts against the base by turning the jam nut clockwise (toward the bottom of the cabinet). Torque the four bolts to 54 - 67 nm (40 - 50 ft-lbs).

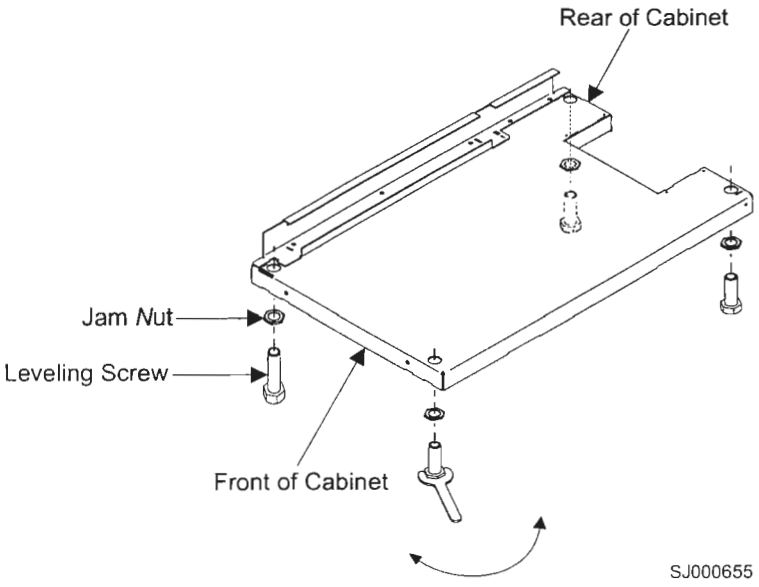


Figure 23. Leveling the cabinet

28. If the cabinet does not have a front door, install the top, left, and right trim panels.

29. After you bolt down the cabinet, go to "Step 7. Attach the front door" on page 16.

Step 6. Attach the mounting plates

Note: You attach the front and rear mounting plates through the same mounting holes that you use to mount the stabilizers. Therefore, you must bolt down the cabinet rather than use the stabilizers. Install the mounting plates *only* if you bolted the cabinet to the floor.

The mounting plates are part of the Earthquake Mounting Kit, feature code 6080.

Align the holes on the mounting plate with the holes on the front of the cabinet. Use the allen wrench that is supplied with the cabinet to install the mounting plate screws (stabilizer mounting screws). Repeat this procedure for the mounting plate on the rear of the cabinet. See Figure 24.

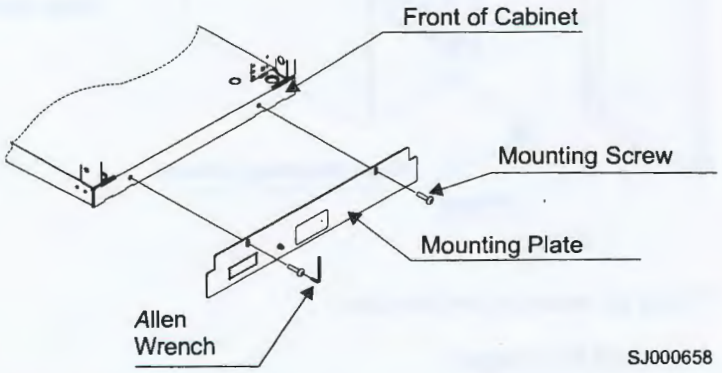


Figure 24. Attaching the mounting plate

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1289
Doc: 3690

Step 7. Attach the front door

If necessary, perform the following steps to attach the front door. Refer to Figure 25 while you perform the steps.

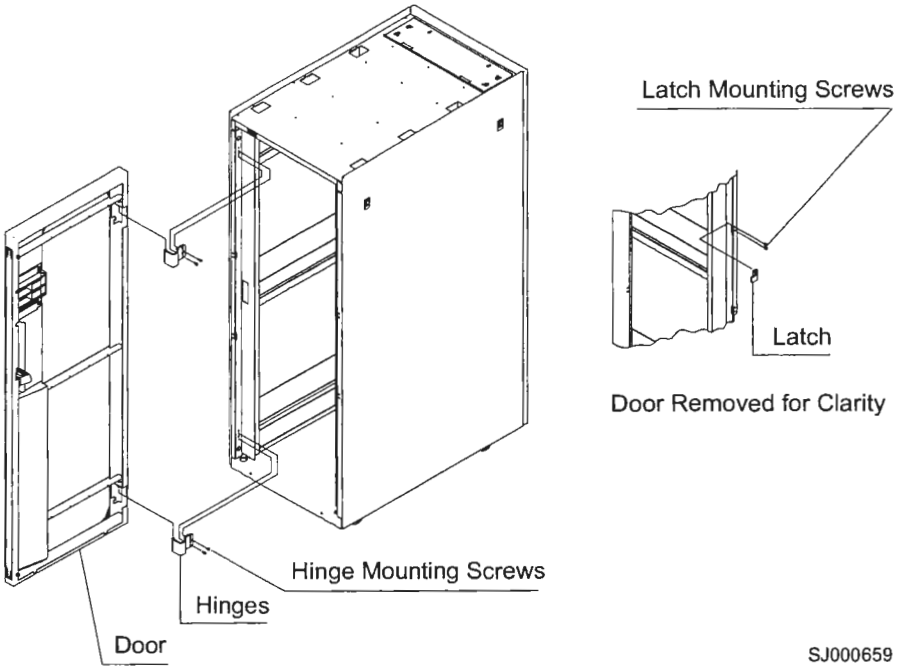


Figure 25. Attaching the front door

1. Install the hinges.
2. Install the latch.
3. Align the lower hinge pin on the front door with the hinge. Partially insert the pin into the hinge.
4. Align the upper hinge pin with the hinge. Lower the door into position.
5. Adjust the latch so that the door is latched securely.

Step 8. Check the customer's ac power source

Before you plug the power cord into the ac power source, perform the following checks on the customer's ac power source.

CAUTION:
Do not touch the receptacle or the receptacle face plate with anything other than your test probes before you meet the requirements in this step.

1. Have the customer turn off the branch circuit breaker for the ac power outlet into which the power cord will plug. Attach a "Do Not Operate" tag (S229-0237) to the circuit breaker switch.

   Note: All measurements are made with the receptacle face plate in the normal installed position.

2. Some receptacles are enclosed in metal housings. For this type of receptacle, perform the following steps:

a. Check for less than 1 volt from the receptacle case to any grounded metal structure, such as a raised-floor metal structure, water pipe, building steel, or similar structure.

b. Check for less than 1 volt from the receptacle ground pin to a grounded point in the building.

Note: If the receptacle case or face plate is painted, be sure that the probe tip penetrates the paint and makes good electrical contact with the metal.

c. Check the resistance from the ground pin of the receptacle to the receptacle case. Check the resistance from the ground pin to the building ground. The readings should be less than 0.1 ohm, which indicates the presence of a continuous grounding conductor.

3. If any of the three checks that you made in step 2 on page 16 are not correct, ask the customer to:
   - Remove the power from the branch circuit.
   - Make the wiring corrections.

   Recheck the receptacle.

   Note: Do not use a digital multimeter to measure grounding resistance in the following steps.
4. Check for infinite resistance between the ground pin of the receptacle and each of the phase pins. This check is for a wiring short to ground or a wiring reversal.
5. Check for infinite resistance between the phase pins. This check is for a wiring short.

   CAUTION:
   If the reading is other than infinity, do not proceed! Have the customer make the necessary wiring corrections before you continue. Do not turn on the branch circuit breaker until you satisfactorily complete all the previous steps.
6. Have the customer turn on the branch circuit breaker. Measure for the appropriate voltages between phases. If no voltage is present on the receptacle case or the ground pin, the receptacle is safe to touch.
7. With an appropriate meter, verify that the voltage at the ac outlet is correct.
8. Verify that the grounding impedance is correct by using the ECOS 1020, 1023, B7106, C7106, or an appropriately approved ground impedance tester.

Step 9. Check the power distribution unit

When the switch power cords are plugged into the power distribution unit (PDU) outlets, resistance should be less than 0.1 ohm between input ground and either switch or cabinet frames.

See "Power distribution unit (PDU)" on page 116 for an illustration and description of the PDU.

External ac power cords

To avoid electrical shock, the manufacturer provides a power cord with a grounded attachment plug. Use only properly grounded outlets.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1290
Doc: 3690

Power cords that are used in the United States and Canada are listed by Underwriter's Laboratories (UL) and are certified by the Canadian Standards Association (CSA). These power cords consist of the following parts:

- Electrical cables, type ST
- Attachment plugs that comply with National Electrical Manufacturers Association (NEMA) L6-30P
- Appliance couplers that comply with International Electrotechnical Commission (IEC) Standard 320, Sheets C13 and C14

Power cords that are used in other countries or regions consist of the following parts:

- Electrical cables, type HD21 or HD22
- Attachment plugs that the appropriate testing organization for the specific countries or regions where they are used has approved
- Appliance couplers that comply with International Electrotechnical Commission (IEC) Standard 320, Sheet C13 and C14

See "Power cords" on page 113 for information about the power cords that are available for the cabinet.

Step 10. Connect switch and device cables

The factory configures the cabinet and installs all of the switch cables.

If you need to install device cables, follow the installation instructions provided with the component that you are installing.

Step 11. Power on the cabinet

See "Power-on procedure" on page 69 for instructions on how to power on the cabinet.

Chapter 3. Starting and configuring the 2109 Model M12

You must configure the 2109 Model M12 appropriately in order for it to operate correctly within the network and fabric.

Note: The 2109 Model M12 only detects modems during power on or restart. If you connect a modem to an operating switch, you must restart the 2109 Model M12 in order for the switch to detect the modem.

This chapter describes how to start and configure the 2109 Model M12 and includes the following information:

- Providing initial power to the chassis
- Configuring, connecting, and accessing the 2109 Model M12

Providing initial power to the chassis

Perform the following steps to provide ac power to the chassis:

1. Connect the cabinet power distribution units (PDUs) to separate power sources of 200 - 240 V ac, 50 - 60 Hz.
2. Make sure that the internal power cords are connected to the separate PDUs and that the other ends are connected to the 2109 Model M12 circuit breakers.
3. Route the power cord so that it is not exposed to stress.
4. Flip both green ac power switches to "|". The ac power switches light up green when switched on, and power is being supplied.

The switch automatically performs a POST by default each time you power it on. A POST takes a minimum of 3 minutes. A POST is complete when light-emitting diode (LED) activity returns to a standard state. For information about LED light patterns, see "Interpreting LED activity" on page 32.

Attention: Do not connect the switch to the network until you configure the IP addresses.

Configuring the 2109 Model M12

The 2109 Model M12 can contain up to two logical switches, each with its own configuration:

- One logical switch for any 16-port cards in slots 1 - 4
- One logical switch for any 16-port cards in slots 7 - 10

The configuration information for both logical switches is stored in the WWN card and in the flash memory of the CP cards. The configuration is automatically mirrored to the standby CP card, so that the most current configuration remains available even if the active CP card fails. You can back up the configuration to a workstation by using the **configUpload** command. You can download the configuration to the active CP card by using the **configDownload** command. For information about commands and whether you can enter them through the active or standby CP card, see the *Brocade Fabric OS Reference*.

Note: You should routinely back up the configuration to ensure that the current configuration is available if needed.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1291
Doc: 3690

© Copyright IBM Corp. 2002, 2003

You can modify the configuration only through a login session to the active CP card. The 2109 Model M12 supports up to two Telnet sessions with administrative privileges at the same time.

The same administrative login account applies to both logical switches. If the password is changed on switch 0, it automatically changes on switch 1.

The 2109 Model M12 configuration includes the following parameters:

- General system parameters

  You can modified these parameters with the **configure** command. For more information, see the *Brocade Fabric OS Reference*.
- WWNs for both logical switches

  You cannot modify the two WWNs. Both of them are preconfigured and are usually based on the chassis-serial number.
- Domain ID

  The default domain ID for both logical switches is 1. You can modify it by using the **configure** command.
- One domain ID for any of the 16-port cards in slots 1 - 4 and one for any of the 16-port cards in slots 7 - 10

  You can modify domain IDs with the **configure** command.
- Native IP addresses

  A native IP address, host name, subnetmask, and gateway address for both CP card slots. You can modify it by using the **ipAddrSet** command.
- Logical IP addresses

  A logical IP address and subnetmask for both logical switches. You can modify it by using the **ipAddrSet** command.

  Note: If you reset a logical IP address while the switch has active IP traffic, you can cause the IP traffic to be interrupted or stopped. IP traffic might include Web Tools, Fabric Watch, SNMP, and other applications.

Items needed

You will need the following items to configure and connect the 2109 Model M12:

- A 2109 Model M12 that is powered on and that is not connected to a network or fabric
- A workstation computer with a terminal emulator application, such as HyperTerminal
- The serial cable that is provided with the 2109 Model M12
- An Ethernet cable
- SFP transceivers and cables, as required
- Two IP addresses for the native IP addresses that are assigned to the CP slots, with the corresponding native host names, subnetmasks, and gateway addresses. The default native IP addresses and host names are as follows:
  - `10.77.77.75 CP0` (the CP card in slot 5 at the time of configuration)
  - `10.77.77.74 CP1` (the CP card in slot 6 at the time of configuration)
- Two IP addresses for the logical IP addresses of the switch, with the corresponding subnetmasks. These IP addresses correspond to "switch 0", which contains any 16-port cards in slots 1 - 4, and "switch 1", which contains any 16-port cards in slots 7 - 10. The default logical IP addresses are as follows:
  - `10.77.77.77 sw0`

- 10.77.77.76 sw1

- Two switch names, if the default switch names are not going to be used. Switch names can be up to 15 characters long. Switch names can include alphabetical, numerical, and underscore characters, and must begin with an alphabetical character. The default switch name for the logical switches is:
  - sw0 for the switch that contains the 16-port cards in slots 1 - 4
  - sw1 for the switch that contains the 16-port cards in slots 7 - 10

Configuration procedure

Note: The following procedure uses various Telnet commands. For information about these commands, see the *Brocade Fabric OS Reference*.

Perform the following steps to configure the 2109 Model M12:

1. Verify that the 2109 Model M12 is on. Verify that the POST is complete by verifying that all power LEDs on the 16-port cards and CP cards display a steady green light. For a description of the LED patterns, see "Interpreting LED activity" on page 32.
2. Login to the CP card that is installed in slot 5 by establishing a serial connection to a workstation that has a terminal emulator application, such as a HyperTerminal in a Microsoft® Windows® 95, Windows 2000, or Windows NT® environment, or TERM in a UNIX® environment.
   a. Disable any serial communication programs that are running on the workstation, such as synchronization programs for a PDA.
   b. Remove the shipping cap from the terminal serial port on the CP card in slot 5 and insert the serial cable. The terminal serial port is the second serial port from the top of the CP card.
   c. Connect the other end of the serial cable to a serial port on the workstation. If necessary, you can remove the adapter on the serial cable to allow for an RJ-45 serial connection.
   d. Open the terminal emulator application and configure as follows:
      - For a Windows 95, 98, 2000, or NT environment, use the configuration parameters shown in Table 2.

Table 2. Configuration parameters

Parameter	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

      - In a UNIX environment, type the following command:

        ```
        tip /dev/ttyb -9600
        ```

   e. When the terminal emulator application stops reporting information, press Enter. The following login prompt displays:

```
CP Console Login:
```

   f. Type the logon information.

The default administrative logon is `admin`, and the default password is `password`.

g. At the prompt, type `0` to log in to switch 0.

```
Enter switch number to login <0 or 1>:0
```

Note: At the initial login, the user is prompted to type a new admin password and a new user password. The same administrative account applies to both logical switches. If the password is changed on switch 0, it automatically changes on switch 1.

h. Change the passwords if desired. Passwords must be a total of 8 - 40 characters long and should include a combination of numbers, uppercase, and lowercase letters. To skip changing the password, press CTRL+C.

3. Type the following command to determine which CP card is active:

   `haShow`

   Information about the card displays. For example:

```
switch:admin> haShow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA Enabled, Heartbeat Up, HA State not in sync
```

4. Configure the IP addresses for both CP cards.

   You can make configuration changes only through a login session with the active CP card. However, you can assign IP addresses to either CP card from a login session with the active CP card.

   a. If the CP card in slot 5 is not the active CP card, disconnect the serial cable from the CP card, connect it to the CP card in slot 6, and login as `admin`.

   b. At the prompt, type `ipAddrSet 2` for the CP card in slot 5, or type `ipAddrSet 3` for the active CP card in slot 6.

   c. Type the requested information at the prompts, as the following example shows. The default information for the CP card in slot 5 is shown.

```
Ethernet IP Address [10.77.77.75]:
Ethernet Subnetmask [255.0.0.0]:
Host Name [CP0]:
Gateway Address [0.0.0.0]:
```

   The host name is the native name that is assigned to the CP card. You must use the same gateway address for both CP cards. These gateway addresses are referenced for the logical IP addresses.

   The native IP address of the active CP card is updated immediately. The native IP address of the standby CP card is updated at the next restart.

   d. Repeat step 4a - step 4c for the other CP card.

5. Configure the two logical IP addresses.

   Note: Resetting a logical IP address while the switch has active IP traffic can cause the IP traffic to be interrupted or stopped. IP traffic might include Web Tools, Fabric Watch, SNMP, and other applications.

If you change the IP address, you can cause a domain address format registered state change notification (RSCN) to be issued.

a. To configure the first logical IP address, type the following command at the prompt:

   ```
   ipAddrSet 0
   ```

b. Type the requested information for this IP address at the prompt:

```
Ethernet IP Address [10.77.77.77]:
Ethernet Subnetmask [0.0.0.0]:
Fibre Channel IP Address [none]:
Fibre Channel Subnet Mask [none]:
```

The logical IP address is updated immediately.

c. To configure the second logical IP address, type the following command at the prompt:

   ```
   ipAddrSet 1
   ```

d. Type the requested information for this IP address at the prompts.

e. At the prompt, type the following command to restart the CP card:

   ```
   reboot
   ```

   Note: You can use the terminal serial port to monitor error messages through a serial connection. Do not use the terminal serial port as a command line interface during normal operations because it only modifies one switch at a time (switch 0 by default).

f. If this port is not used continuously, remove the serial cable. Replace the shipping cap to protect the port from dust.

6. Optional: Connect the active CP card by Ethernet cable to the local area network (LAN).

   a. Remove the shipping plug from the Ethernet port on the active CP card.

   b. Insert one end of an Ethernet cable into the Ethernet port.

   c. Connect the other end to an Ethernet 10/100BASE-T LAN.

   You can now access the switch remotely by using any of the available management tools, such as Telnet or Web Tools. Be sure that the switch is not modified from other connections during the rest of this procedure.

7. Optional: Login to either of the logical switches by Telnet, using the administrative logon. The default administrative logon name is `admin`, and the default password is `password`.

   You can now access the switch remotely using Telnet or Web Tools. Be sure that the switch is not being modified from any other connections during the remaining steps. The 2109 Model M12 supports up to two Telnet sessions with administrative privileges at the same time. You can accomplish the remaining steps in this procedure with either a serial connection or a Telnet session.

8. Optional: Customize the switch names for the logical switches, if desired. If possible, use the default switch names.

   Note: Changing the name of the switch causes a domain address format RSCN to be issued.

   a. Type `switchName`, with the new switch name enclosed in double quotation marks. In the following example, `"sw10"` is the new switch name.

      ```
      switchName "sw10"
      ```

ECT
POS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1293
Doc: 3690

b. Record the new switch name for future reference.

c. To customize the switch name for the other logical switch, perform the following steps:

   1) Log out from the CP session.

   2) Connect the serial cable to the other CP card.

   3) Log in as admin.

   4) Repeat step 8a on page 23 and step 8b for the other logical switch.

9. Optional: Modify the domain IDs, if desired.

   Type `fabricShow` to see a list of the current domain IDs.

   Note: The default domain ID for both switches is 1. To prevent a domain ID conflict, make the domain IDs unique before you connect the switches to the fabric.

   a. Type the following command to disable the switch:

      `switchDisable`

   b. Type the following command:

      `configure`

   c. Type `y` at the `Fabric parameters` prompt:

```
Fabric parameters (yes, y, no, n): [no] y
```

   d. Type a unique domain ID at the `Domain` prompt:

```
Domain: (1..239) [1] 3
```

   e. Complete the remaining prompts or press CTRL+D to accept the other settings and exit.

   f. Type the following command to re-enable the switch:

      `switchEnable`

10. Optional: Specify any custom status policies.

   a. To access the status policy, type the following command at the prompt:

      `switchStatusPolicySet`

   b. Complete the prompts to specify the status policies. To completely deactivate the alarm for a particular condition, type `0` at the prompt for that condition.

11. Add SFPs and cables to the Fibre Channel ports, as required.

   Note: The ports are color-coded to indicate which ones can be used in the same trunking groups. Four ports that are marked with black solid ovals alternate with four ports that are marked with oval outlines. The ports and cables that are used in trunking groups must meet specific requirements. For a list of these requirements, see the *IBM TotalStorage SAN Switch 2109 Model M12 User's Guide* and the *Brocade ISL Trunking User's Guide*.

   a. Position one of the SFPs so that the key is oriented correctly to the port. Insert the SFP into the port until it is firmly seated. Ensure that the latching mechanism clicks.

      Note: SFPs are keyed so that you can only insert them with the correct orientation. If an SFP does not slide in easily, ensure that it is

correctly oriented. For instructions that are specific to the SFP model, see the documentation of the SFP manufacturer.

b. Position a cable so that the key (the ridge on one side of the cable connector) aligns with the slot in the SFP. Insert the cable into the SFP until the latching mechanism clicks.

   Note: Cables are keyed so that you can only insert them with the correct orientation. If a cable does not slide in easily, ensure that it is correctly oriented.

c. Repeat step 11a on page 24 and step 11b for the remaining ports.

d. Organize the cables as required.

12. Check the 2109 Model M12 for switch and port status. Type the following command at the Telnet prompt:

    `switchShow`

    This command provides detailed information about the switch.

13. Check the fabric for ISLs, switch names, or other status. Type the following command at the Telnet prompt:

    `fabricShow`

    This command provides general information about the fabric.

14. After all zoning configurations and other changes are complete, back up the configuration. Type the following command at the Telnet prompt:

    `configUpload`

    This command uploads the switch configuration to the server, so that it is available for downloading to a replacement switch if necessary.

    Note: You should routinely back up the configuration.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1291
Doc: 3690

Chapter 4. Operating the 2109 Model M12

This chapter describes how to operate the 2109 Model M12 and includes the following information:

- Turning on and off the 2109 Model M12
- Interpreting LED activity
- Interpreting POST
- Maintaining the switch

Note: Throughout this chapter, the term *switch* refers to the 2109 Model M12.

Turning on and off the 2109 Model M12

Note: To provide power to the switch for the first time, see "Power-on procedure" on page 69.

To turn on the 2109 Model M12, verify that both power cords connect to the ac power connectors on the front of the chassis. Flip both green ac power switches to "|". The green ac power switches illuminate when they are on.

To turn off the 2109 Model M12, flip both ac power switches to "O": To remove all sources of power from the switch, disconnect both power cords from the power source.

Note: Removing all power from the switch triggers a system reset. When you restore the power, all devices return to the initial state, and the switch runs a POST.

Attention: After you power on the 2109 Model M12, run it for a minimum of 10 minutes before you power off again.

Switch components

The 2109 Model M12 includes the following components:

- 16-port cards
- CP cards
- Power supplies
- ac power input connection
- ac power switches
- Blower assemblies
- WWN card and bezel
- Cable management tray

RQS nº 03/2005 - CN - CPMI--- CORREIOS
Fls.. Nº 1295
Doc: 3690

© Copyright IBM Corp. 2002, 2003

16-port cards

Attention: Wear an electrostatic discharge (ESD) grounding strap when you work with a 16-port card to prevent damage to the electrical components.

To ensure correct cooling of the chassis and protection from dust, install a filler panel in any slots that do not contain a 16-port card.

Disassembling any part of a 16-port card voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the 16-port card.

Each 16-port card provides 16 auto-sensing Fibre Channel ports that are capable of auto-sensing data transmission speeds of 1 Gbps and 2 Gbps.

You can install 16-port cards in any combination of slots 1 - 4 (switch 0) and 7 - 10 (switch 1), with one exception. If there are one or more 16-port cards in slots 7 - 10, there must be at least one 16-port card in slots 1 - 4.

The ports on each of the 16-port cards are color-coded. The color code indicates which ports to use in the same ISL Trunking group. Four ports that are marked with black solid ovals alternate with four ports that are marked with oval outlines.

Note: ISL Trunking is a Fabric OS feature. ISL Trunking enables distribution of traffic over the combined bandwidth of up to four ISLs between two directly adjacent switches, while preserving in-order delivery. For more information about ISL Trunking, see the *Brocade ISL Trunking User's Guide*.

The 2109 Model M12 can continue to operate while you replace a 16-port card, but you must disconnect any devices that are connected to the 16-port card. To ensure correct air circulation inside the switch and protection from dust, you can order filler panels for any empty slots.

Perform the following steps to determine the status of a 16-port card:

1. Check the LEDs on the 16-port card. See Table 3 on page 33 for information about how to interpret the LEDs.
2. Check the 16-port card status by using the **slotShow** command. For additional information about this command, see the *Brocade Fabric OS Reference*.

Control processor cards

Attention: Wear an ESD grounding strap when you work with a CP card to prevent damage to the electrical components.

To ensure correct cooling of the chassis and protection from dust, install a filler panel in any slots that do not contain a CP card.

Disassembling any part of a CP card voids the part warranty and regulatory certifications. No user-serviceable parts are inside the CP card.

High availability is provided through redundant CP cards: An active CP card and a standby CP card. The active CP card is the one that is actively controlling the 2109 Model M12. If the active CP card failed or is uninstalled, the standby CP card

automatically becomes the new active CP card. Failover occurs as soon as the active CP card is detected to be faulty or uninstalled.

Information about both CP cards, including which card is active, is available by using the **haShow** command. For information about commands and whether you can enter them through the active or standby CP card, see the *Brocade Fabric OS Reference*.

Each CP card provides the following ports:

- Modem serial port

  The modem serial port has an RS-232 connector that is wired as a data terminal equipment (DTE) device. It is designed to connect to a distributed computing environment (DCE) device, such as a modem.
- Terminal serial port (also known as a console port)

  The terminal serial port has an RS-232 signal subset connector that you can use to connect to a PC serial port or dumb terminal.
- Ethernet port

  The Ethernet port has an RJ-45 connector and is capable of speeds of 10 Mbps or 100 Mbps.

You can connect a separate modem to each modem serial port, and then connect to the same or separate telephone lines for redundancy.

Note: The 2109 Model M12 only detects modems during power on or restart. If a modem is connected to an operating switch, you must restart the 2109 Model M12 in order to detect the modem.

The 2109 Model M12 can continue to operate while a CP card is being replaced. To ensure correct air circulation inside the switch and protection from dust, you can order filler panels for any empty slots.

The active CP card controls the following services:

- System initialization
- High availability and switch drivers
- Name server
- SNMP
- Fabric OS
- Extended Fabrics
- Fabric Watch
- Remote Switch
- Web Tools
- Zoning

Perform the following steps to determine the status of a CP card:

1. Check the LEDs on the CP card. See Table 4 on page 37 for information about how to interpret the LEDs.
2. Check the CP card status by using the **slotShow** and **haShow** commands.

   For additional information about these commands, see the *Brocade Fabric OS Reference*.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1296
Doc: 3690

Power supplies

The 2109 Model M12 uses four power supplies. A minimum of two power supplies is required to power a completely loaded chassis.

The 2109 Model M12 can continue operating while a power supply is being replaced if at least one power supply continues operating for every four 16-port cards that are installed. You must have a minimum of two power supplies.

Attention: To protect against ac failure, you must have a minimum of one power supply in slot 1 or slot 3 and one in slot 2 or slot 4. If you install only two power supplies and you install both of them in slots that correspond to the same power cable, unplugging a single power cable will power down the entire chassis.

Attention: Disassembling any part of the power supply voids the part warranty and regulatory certifications.

Attention: Before you replace a power supply, determine whether adequate power will be available to keep the chassis operating throughout the replacement. If not, shut down both switches before you continue. If adequate power is abruptly lost, such as through removal of a power supply, the entire switch is powered down. The power off order that is designated by the **powerOffListSet** command is not followed.

CAUTION:
No user-serviceable parts are inside the power supply.

Perform the following steps to determine the status of a power supply:

1. Check the LEDs on the power supply. See Table 5 on page 39 for information about how to interpret the LEDs.
2. Check the power supply status by using the **psShow** command. The power supply status displays OK, absent, or faulty. For additional information about the **psShow** command, see the *Brocade Fabric OS Reference*.

ac power input connectors and ac power switches (circuit breaker)

The 2109 Model M12 has two ac power input connectors, each with a green ac power switch (circuit breaker). The left power input connector provides power to the power supplies in slot 1 and slot 3. The right power input connector provides power to the power supplies in slot 2 and slot 4. The power input connectors and their associated power supplies are color-coded.

Attention: Unplugging a single power cable can power down the entire switch, depending on which power supply slots contain power supplies.

Two detachable power cords are provided with the cabinet and are customized for the country or region in which it is installed.

The ac power switches light up green when they are on.

Blower assemblies

Three blower assemblies that are located in the back of the chassis cool the 2109 Model M12. The air enters through the vents in the blower assembly side of the chassis. The air exits from the top vent on the port side of the chassis. Each switch requires a minimum airflow of 350 cubic feet per minute.

The blower assemblies are hot-swappable if two blower assemblies remain operating. If you remove more than one blower assembly at the same time, turn off the 2109 Model M12 to prevent overheating.

Note: The 2109 Model M12 requires a minimum of two functioning blower assemblies during operation. To ensure continuous adequate cooling, maintain three operating blower assemblies at all times except for the brief period when replacing a blower assembly. The 16-port cards automatically shut down if the temperature range is exceeded.

Attention: Disassembling any part of the blower assembly voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the blower assembly.

Perform the following steps to determine the status of a blower assembly:

1. Check the LEDs on the blower assembly.
2. Check the blower assembly status by using the **fanShow** command. The status for each blower assembly displays OK, absent, or faulty. For additional information about the **fanShow** command, see the *Brocade Fabric OS Reference*.

WWN card and bezel

The WWN card and bezel are located at the top of the chassis on the blower assembly side. The WWN card has LEDs that you use to monitor the 2109 Model M12. The WWN card also stores the following information:

- The chassis serial number (used when installing software licenses)
- The two native IP addresses that are assigned to the CP card slots
- The logical switch names, IP addresses, and WWNs for the two logical switches

The bezel protects the card and identifies each of the LEDs on the WWN card. Together, the WWN card and bezel assembly provides a consolidated view of the LEDs for the two CP cards, eight 16-port cards, and four power supplies. If a slot contains a filler panel, the corresponding LEDs on the WWN card are not illuminated.

Note: There are two types of WWN cards. One type is attached to the chassis by screws and the other type is held on by the pressure of the bezel against a pad on the card face.

Attention: Although the information that is stored in the WWN card is also stored in the flash memory of the CP cards, do not restart the switch while the WWN card is uninstalled. Restarting the switch can cause the switch to start incorrectly.

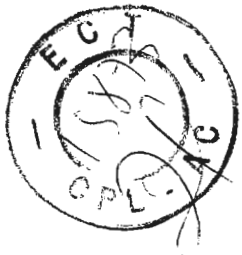
Attention: Wear an ESD grounding strap when you work with the WWN card to prevent damage to the electrical components.

Cable management items

Two items are provided to assist with cable management:

- Cable management tray

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1297
Fls. Nº
Doc: 3690



The cable management tray is attached to the bottom of the chassis. You can use it to route the power cables and other cables down below the chassis or out the sides of the chassis.

- Cable guides

  A set of 16 cable guides is provided with the cabinet. You can use the guides to organize the port cables into logical groups, such as according to port quads (sets of four neighboring ports). The cable guides are free-floating and do not attach to the chassis. The cable guides keep the cables evenly spaced and hold them away from the 16-port cards. This makes card replacement easier and prevents the cables from bending to less than the minimum bend radius.

  Attention: Do not route the cables in front of the air exhaust vent, which is located at the top of the port side of the chassis.

  The minimum bend radius for a 50-micron cable is 3.05 cm (2 in.) under full tensile load, and 3.048 cm (1.2 in.) with no tensile load.

  Do not use tie wraps for optical cables because they are easily overtightened.

Interpreting LED activity

You can determine system activity and status by monitoring the activity of the LEDs on the switch.

There are four possible LED states:

- No light
- Steady light in one of the following colors:
  - Green
  - Amber
  - Yellow (displays when both green and amber LED elements are lit)
- Slow-flashing light (green, amber, or yellow)
- Fast-flashing light (green, amber, or yellow)

The LEDs can flash green, yellow, or amber while the switch is starting or while a POST or other diagnostic tests are running. This is normal. It does not indicate a problem unless the LEDs do not indicate that all components are operational after the switch is started, after a POST, or after any diagnostic tests are complete.

See the error log for any errors. For information about the error log, see the *Brocade Diagnostic and System Error Message Reference*.

LEDs on the 16-port card

The following LEDs are on the 16-port card:

- Power LED
- Status LED
- Port status LED for each port
- Port speed LED for each port

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

Figure 26 on page 33 shows the location of the LEDs on the 16-port card.

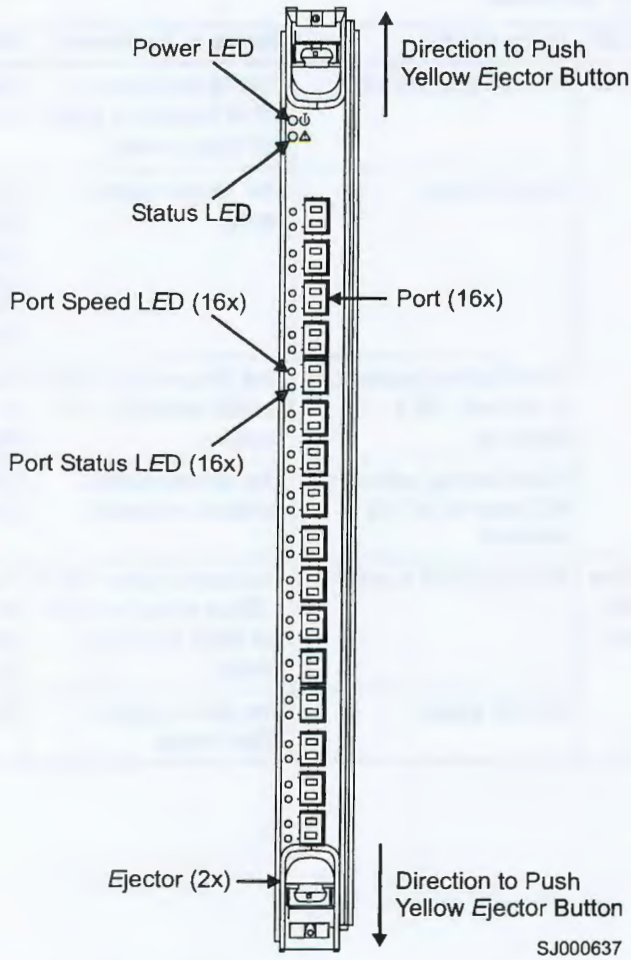


Figure 26. 16-port card LEDs

Table 3 describes the 16-port card LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and the action that you can take in response to that status.

Table 3. 16-port card LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Uppermost LED	No light (LED is off)	The 16-port card does not have incoming power.	Ensure that the card is firmly seated and has power.
		Steady green	The 16-port card has incoming power.	No action is required.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1298
Doc: 3690

Table 3. 16-port card LED patterns (continued)

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Status	Below the Power LED	No light (LED is off)	The 16-port card is either healthy or does not have power.	Verify that the Power LED is lit.
		Steady yellow	The 16-port card is faulty.	Ensure that the card is firmly seated and check the status with the **slotShow** command. If the LED still displays yellow, contact IBM.
		Slow-flashing yellow (on 2 seconds; off 2 seconds)	The 16-port card is not seated correctly, or is faulty.	Pull the card out and reseat it. If the LED continues to flash, replace the card.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	The environmental range is exceeded.	Check for out-of-bounds environmental condition.
Port Speed	Uppermost of the two LEDs to the left of each port	No light (LED is off)	The port is either set to 1 Gbps mode, or does not have incoming power.	Verify that the Power LED is lit. To change the mode, see the *Brocade Fabric OS Procedures Guide*.
		Steady green	The port is set to 2 Gbps mode.	No action is required.

Table 3. 16-port card LED patterns (continued)

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Port Status and Activity	To the left of each port, below the Port Speed LED	No light (LED is off)	• Either the 16-port card does not have incoming power or there is no light or signal carrier detected. • Polling is in progress. • The connected device is configured in an offline state.	Verify that the Power LED is lit and check the transceiver and the cable.
		Steady green	The port is online (connected to an external device) but has no traffic.	No action is required.
		Slow-flashing green (on 1 second; off 1 second)	The port is online but segmented, indicating a loopback plug or cable, or an incompatible switch.	Verify that the correct device is connected to the port.
		Fast-flashing green (on 1/4 second; off 1/4 second)	The port is in internal loopback (diagnostic).	No action is required.
		Flickering green	The port is online, with traffic flowing through the port.	No action is required.
		Steady yellow	The port is receiving light or signal carrier, but is not yet online.	No action is required.
		Slow-flashing yellow	The port is disabled (from diagnostic tests or the **portDisable** command).	Reset the port from the workstation.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	The SFP or the port is faulty.	Change the SFP or reset the switch from workstation
		Alternating green and yellow	The port is bypassed.	Reset the port from the workstation.

LEDs on the CP card

The following LEDs are on the CP card:

- Power LED
- Status LED
- Link status and activity LED
- Link speed LED

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1299
Doc: 3690

Figure 27 shows the location of the LEDs on the CP card.

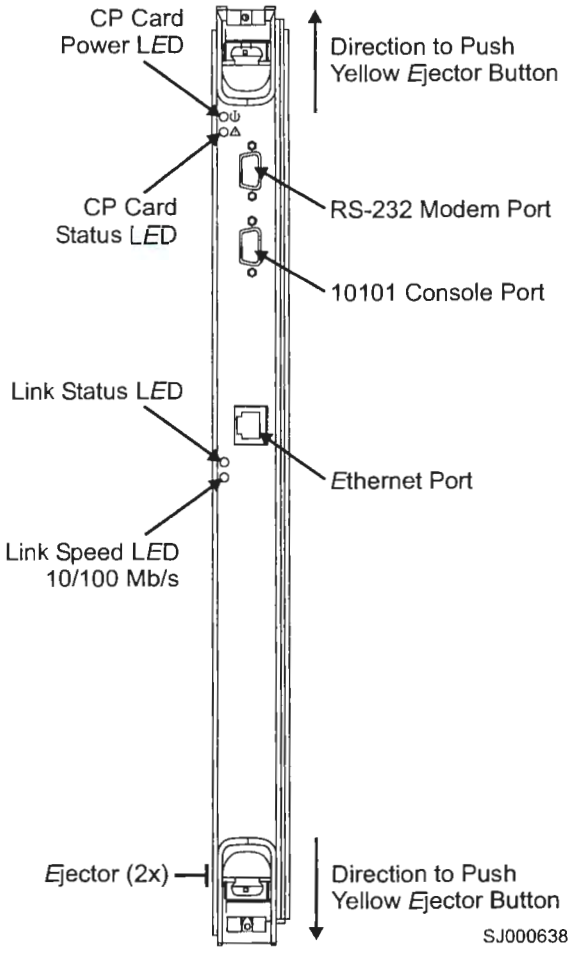


Figure 27. CP card LEDs

Table 4 describes the CP card LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and action that you can take in response to that status.

Table 4. CP card LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Uppermost LED	No light (LED is off)	The CP card does not have incoming power.	Ensure that the CP card is firmly seated and has power.
		Steady green	The CP card has incoming power.	No action is required.
Status	Below the Power LED	No light (LED is off)	The CP card is either healthy or does not have incoming power.	Verify that the Power LED is lit.
		Steady yellow	The CP card is faulty.	Ensure that the CP card is firmly seated. If the LED still displays yellow, contact IBM.
		Slow-flashing yellow (on 2 seconds; off 2 seconds)	The CP card is not seated correctly, or is faulty.	Pull the CP card out and reseat it. If the LED continues to flash, replace the CP card.
		Fast-flashing yellow (on 1/2 second; off 1/2 second)	The environmental range is exceeded.	Check for out-of-bounds environmental condition.
Link status and activity (labeled "Link" on the CP card)	Uppermost of the two LEDs below and to the left of the Ethernet port	No light (LED is off)	Either the CP card does not have incoming power or no link is detected.	Ensure that the CP card has power. Verify that the Ethernet cable is firmly seated and the device at the other end of the link is functioning.
		Flickering green and yellow	The link is healthy, with traffic flowing through the port.	No action is required.
Link speed (labeled "10/100 Mb/s" on the CP card)	To the left of the Ethernet port, below the Link status and activity LED	No light (LED is off)	Either the link speed is 10 Mbps or the CP card does not have incoming power.	Ensure that the CP card has power.
		Steady green	The link speed is 100 Mbps.	No action is required.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1300
Fls. Nº
Doc: 3690

LEDs on the power supply

The following LEDs are on each power supply:

- Power LED
- Predictive Failure LED
- Fail LED

If only one ac power switch is turned on, the fail LED on each of the two power supplies without power lights up.

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

Figure 28 shows the location of the LEDs on the power supply.

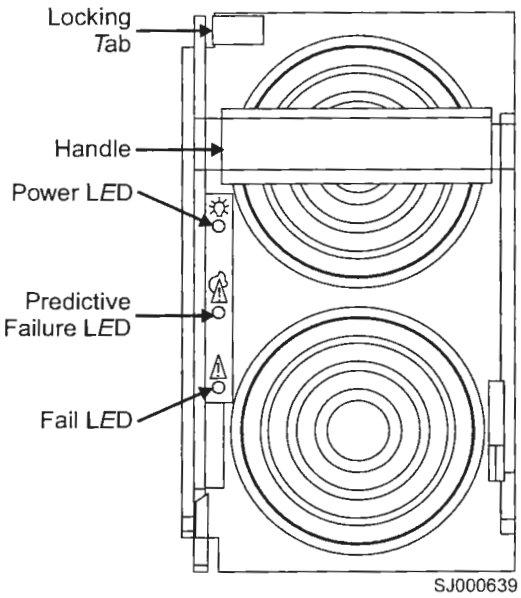


Figure 28. Power supply LEDs

Table 5 on page 39 describes the power supply LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and action that you can take in response to that status.

Table 5. Power supply LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Uppermost LED	No light (LED is off)	The power supply does not have incoming power.	Ensure the following: • The power supply is firmly seated. • The switch has incoming power. • Both power cables are connected. • The ac power switches are on.
		Steady green	The power supply has incoming power and is providing power to the switch.	No action is required.
Predictive Failure	Below the Power LED	No light (LED is off)	The power supply is either healthy or does not have incoming power.	Check the Power LED.
		Flashing amber	The power supply is about to fail because there is a failing fan inside the power supply.	Replace the power supply.
Fail	Below the Predictive Failure LED	No light (LED is off)	The power supply is either healthy or does not have incoming power.	Check the Power LED.
		Steady amber	Either the switch has power but this power supply does not (ac switch might be off), or the power supply has failed.	Ensure that the correct ac power switch is on and the power supply is seated. If the LED still displays, replace the power supply.
		Flashing amber	The power supply is unable to supply power.	Verify that the incoming power meets the requirements listed in "Power specifications" on page 103.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1301
Doc: 3690

LEDs on the blower assembly

The following LEDs are on each blower assembly:

- Power LED
- Fault LED

Figure 29 shows the location of the LEDs on the blower assembly.

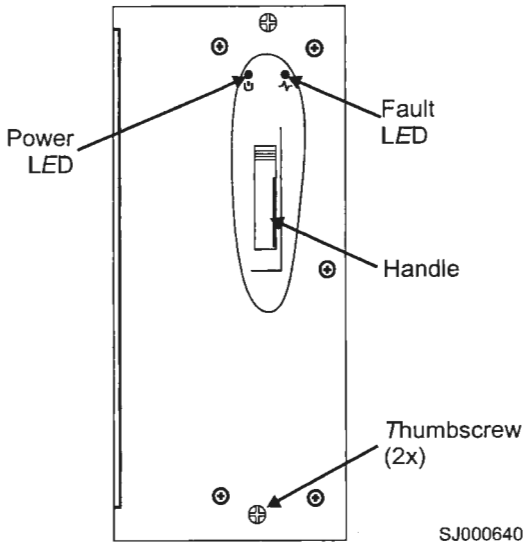


Figure 29. Blower assembly LEDs

Table 6 describes the blower assembly LED patterns. It lists the name, location, and possible colors of each LED. It also lists the status of the switch that is associated with each LED color and action that you can take in response to that status.

Table 6. Blower assembly LED patterns

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Power	Above and to the left of the blower assembly handle	No light (LED is off)	The blower assembly does not have incoming power.	Ensure that the blower assembly is firmly seated and has power.
		Steady green	The blower assembly has incoming power.	No action is required.

Table 6. Blower assembly LED patterns (continued)

Name of LED	Location of LED	Color of LED	Status of hardware	Action
Fault	Above and to the right of the blower assembly handle	No light (LED is off)	The blower assembly is either healthy or does not have incoming power.	Ensure that the blower assembly has incoming power.
		Steady amber	The blower assembly has fully or partly failed.	Replace the blower assembly.
		Slow-flashing amber (on 2 seconds; off 2 seconds)	The blower assembly is not seated correctly or is faulty.	Pull out the blower assembly and reseat it. If the LED continues to flash, replace the blower assembly.
		Fast-flashing amber (on 1/2 second; off 1/2 second)	The environmental range is exceeded.	Check for an out-of-bounds environmental condition, resolve any problems, then reseat unit. If the LED continues to flash, replace the unit.

LEDs on the WWN card and bezel

The WWN card and bezel are located at the top of the chassis on the blower assembly side. The bezel covers the WWN card, allowing the LEDs to shine through. The WWN card and bezel provides a consolidated LED view of:

- The incoming power to and status of the 16-port cards in slots 1 - 4 and 7 - 10
- The incoming power to and status of the CP cards in slots 5 and 6
- The incoming power to the four power supplies

If a slot has a filler panel in place of a 16-port card, a CP card, or a power supply, the LEDs for that slot on the WWN card and bezel do not light up.

If a Status or Fail LED on the power supply flashes, the Power LED on the WWN card also flashes for increased visibility.

Note: The LED patterns can temporarily change during a POST and other diagnostic tests.

Figure 30 on page 42 shows the location of the LEDs on the WWN card and bezel.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1302
Doc: 3690

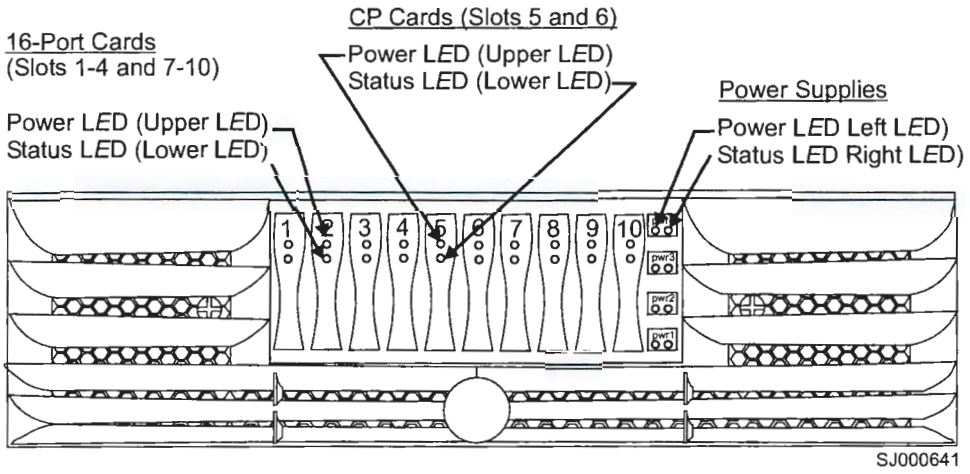


Figure 30. LEDs on the WWN card and bezel

Interpreting POST

The 2109 Model M12 performs a POST by default each time the chassis is powered on (cold start) or started. You can restart the 2109 Model M12 with the **switchReboot, reboot,** or **fastboot** commands. The **fastboot** command restarts the switches without running a POST. A CP card failover event results in a restart for the affected CP card.

POST includes a number of diagnostic tests. You can monitor the test results through LED activity, the error log, or the command line interface. POST requires a minimum of 3 minutes to complete (the time varies and depends on the devices that are connected to the 2109 Model M12).

POST includes the following steps:

1. Running preliminary POST diagnostics
2. Initializing the operating system
3. Initializing the hardware
4. Running diagnostic tests on a number of functions, including:
   - Internal connections and circuitry
   - Port function
   - Ability to send and receive frames
   - All aspects of memory, parity, and statistics counters
   - Correct serialization

The following switch initialization steps are performed whether or not a POST runs:

1. Configures the universal port.
2. Initializes the links.
3. Analyzes the fabric. If any ports connect to other fabric elements (switches), the switch participates in a fabric configuration.
4. Obtains a domain ID and assigns port addresses.
5. Constructs unicast routing tables.
6. Enables normal port operation.

Perform the following steps to verify that a POST completes without errors:

1. Verify that all LEDs return to a normal state after a POST completes. If one or more LEDs do not return to a normal state, and this is not due to the switch being set to beacon, see "Interpreting LED activity" on page 32. Run the **slotShow** command to check the status of the slots.
2. Verify that the switch prompt displays when a POST completes. If it does not display, a POST did not successfully complete. Contact IBM for support.
3. Review the system log. Any errors that are detected during a POST are written to the system log. You can view this error log by running the **errShow** command.

For information about error messages or how to set a switch to beacon, see the *Brocade Diagnostic and System Error Message Reference* and the *Brocade Fabric OS Reference*.

Maintaining the switch

The 2109 Model M12 does not require any regular physical maintenance. It is designed to minimize the chance of failure by using diagnostic tests and field replaceable units (FRUs).

Diagnostic tests

Diagnostic tests are provided to help you to identify problems in the hardware and the firmware. The diagnostic tests include tests of internal connections and circuitry, SFPs, and fiber-optic cables in use. You can run the tests either by using Telnet or through a terminal that is set up for a serial connection to the switch. Some tests require that external cables connect the ports to each other. This allows diagnostics to verify the serializer or deserializer interface and to test the attached SFP and cable.

All diagnostic tests run at link speeds of 1 Gbps and 2 Gbps. For information about diagnostic tests and how to run them, see the *Brocade Fabric OS Reference*.

Note: The diagnostic tests temporarily lock the transmit and receive speed of the links to a specific speed.

Field replaceable units

You can replace the 16-port cards, CP cards, power supplies, and blower assemblies in the field without special tools. In most cases, the switch can continue to operate while you replace a field replaceable unit (FRU). See Chapter 7, "Servicing the 2109 Model C36 with Model M12", on page 69 for the detailed procedures for how to replace these FRUs and other components.

You can configure Fabric Watch alarms for each FRU. For information about Fabric Watch alarms, see the *Brocade Fabric Watch User's Guide*.

You can determine the status of the individual FRU by visually checking the LEDs on the hardware components (see "Interpreting LED activity" on page 32) or by using Telnet commands. For information about Telnet commands, see the *Brocade Fabric OS Reference*.

RQS nº 03/2005 - CN -
CPMI – CORREIOS
Fls. Nº 1303
Doc: 3690

Environmental status and maintenance commands

You can also view environmental information and switch status by using Telnet commands. See the *Brocade Fabric OS Reference* for a complete description of these commands.

Chapter 5. Installing modems

Each CP card in the 2109 Model M12 contains a modem serial port that allows you to connect to a Hayes-compatible modem. The modem serial port is wired as a standard DTE port. You do not need any additional software on the 2109 Model M12 to use the modems.

The modem serial port has the same command, login capabilities, and operational behavior as the terminal serial port. However, asynchronous informational messages and other unsolicited text are not sent to the modem ports.

Connecting a separate modem to each CP card and then connecting both modems to a shared telephone line ensures the high availability of the modem connection. This ensures that one telephone line is used to access the active CP card when a failover occurs. You must log in again if a failover occurs. If both CP cards connect to a shared telephone line, callers automatically dial into the active CP card. The active CP card answers on the first ring. If the active CP card cannot answer for any reason, the standby CP card answers on the seventh ring and allows a login to proceed.

Note: The 2109 Model M12 detects modems only during power-on, restart, or a CP card failover sequence.

After you connect the modems, you can use a Telco system to dial-in to the modems and verify that they answer and dialogue as expected. If a dial-out modem facility is not available, you can use a terminal emulation program on a computer workstation (or laptop) that has an attached modem. See "Setting up a remote modem system (optional)" on page 46 for instructions on how to set up a remote modem for testing purposes. For security reasons, the modem session is automatically disconnected if the modem cable is detached while a session is active.

Figure 31 on page 46 shows two modems that are connected to a 2109 Model M12.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1304
Doc: 3690

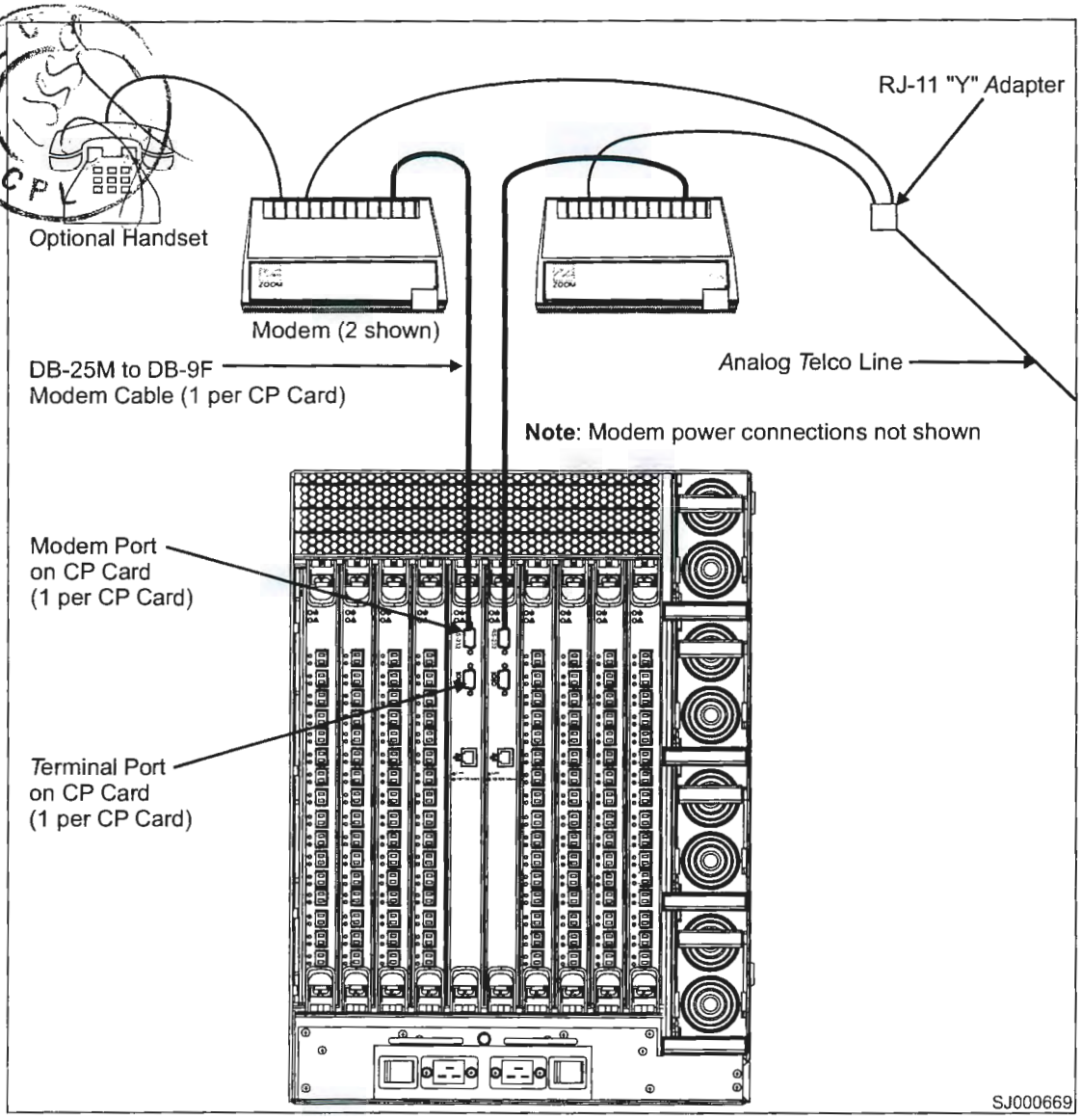


Figure 31. 2109 Model M12 with two modems connected

Setting up a remote modem system (optional)

Note: You should set up the modems before you power on the 2109 Model M12 and connect it to the fabric.

This section provides information about how to set up a remote modem for testing the 2109 Model M12 modems.

Perform the following steps to set up the optional remote modem system:

1. Connect the remote modem to a computer workstation that has a terminal emulator application such as HyperTerminal on Windows 95, 98, 2000, ME or NT, or TERM in a UNIX environment.
2. Disable any serial communication programs that are running on the workstation, such as synchronization programs for a personal digital assistant (PDA).

3. Start the terminal emulator application and if needed, configure as follows:
   - Enter the parameters in Table 7 for Windows 95, 98, 2000, ME, or NT, or TERM in a UNIX environment.

Table 7. Modem parameters for Windows 95, 98, 2000, ME, or NT, or TERM in a UNIX environment

Parameter	Value
Port speed (bits per second)	115200. This value usually defaults to the highest speed that the modem supports and then possibly negotiates for a slower speed.
Data protocol	Standard EC
Compression	Enabled
Flow control	Hardware
Databits	8
Parity	None
Stop bits	1
Modulation	Standard

   - For most UNIX systems, at the prompt, type:

     ```
     tip /dev/ttyb -9600
     ```

4. Follow the instructions from the modem manufacturer for setting up and verifying the modem operation.

Installing the modems on the 2109 Model M12

Note: You should set up the modems before you power on the 2109 Model M12 and connect it to the fabric.

The 2109 Model M12 detects modems only during power on, restart, or CP card failover. Set up the modems before you connect the 2109 Model M12 to the fabric.

You need the following items to set up two modems to work with the 2109 Model M12:

- Two Hayes-compatible modems, such as the Zoom/Modem V.92 EXT Model 3049
- Two standard modem cables, DB25 (male) to DB9 (female)
- One RJ-11 Y adapter for standard Telco wiring or equivalent circuitry (a total of three connections)
- One analog telephone line

CAUTION:
For normal installation, the 2109 Model M12 and attached modems are powered off before cabling them. The modems are automatically detected during a power-on sequence.

Perform the following steps to install the modems:

1. Verify that the power to the 2109 Model M12 is off.
2. Set up the two modem units and the required power connections. Do not turn on the power to the modems until all cables are attached.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1305
Fls. Nº
3690
Doc:

3. Connect the modem cables to the modems and to the 2109 Model M12 modem ports. See Figure 31 on page 46.
4. Connect the telephone line inputs on the modems to the RJ-11 *Y* adapter. This effectively places both modems on a single telephone line.
5. Optional: Connect a telephone handset to one of the telephone connections on the modem. See Figure 31 on page 46.
6. Connect the RJ-11 *Y* adapter to an appropriate analog telephone line.

   Note: Write down the dial-in number. You will use this number later.
7. Turn on the power to the modems. Verify that the modem-ready (MR) indicators light on both modems.
8. Power on the 2109 Model M12, or restart it if you did not power off during the previous steps. Performing this step allows the 2109 Model M12 to recognize the modems.

Verifying modem installation

Perform the following steps to verify that the modems are installed correctly:

1. Verify that both modem cables are connected at the modem and the CP card.
2. Turn on the power to the modems if not already on.
3. Turn on the power to the 2109 Model M12 if not already on.
4. Verify that both modems are ready by checking the following LEDs:
   - Clear to send (CS)
   - Terminal ready (TR)
   - Modem ready (MR)

   If the LEDs do not light, ensure that the modems are connected to a power source and have the power turned on. Also recheck the modem cable connections on the modem and the modem port of the 2109 Model M12.
5. Wait until a POST completes on the 2109 Model M12 (a minimum of 3 minutes).
6. Using a remote client dialing facility (as described in "Setting up a remote modem system (optional)" on page 46), dial in to the customer telephone number for the 2109 Model M12.
7. Observe the modem LEDs. The ring indicator (RI) LED should flash briefly as the telephone rings. If the RI LED does not flash on both modems, recheck the incoming telephone lines to the modems.
8. After one ring, the off hook (OH) LED on the modem that is associated with the active CP card (usually in slot 5) should light. A login prompt displays to the remote client. Login normally.

   Note: If the OH LED on the standby CP card (usually in slot 6) lights after seven rings, recheck the active modem cable connections of the CP.
9. Disconnect the modem session of the active CP card that is using the remote client software.
10. Remove the Telco connector from the active CP card modem. Leave the Telco line of the standby CP card connected to the RJ-11 *Y* adapter. See Figure 31 on page 46.
11. Using the remote client dialing facility, dial in to the customer telephone number for the 2109 Model M12.

12. Observe the modem LEDs carefully. The RI LED should now flash only on the modem that is connected to the standby CP card.
13. After seven rings, the OH LED on the modem that is associated with the standby CP card should light. A login prompt displays to the remote client. A message confirms that the standby CP card is being logged into. Login normally, if desired, or disconnect the session.
14. Restore the Telco connector to the active CP card modem.

The 2109 Model M12 modems are now ready to use.

Notes:

1. Experienced users can use the **haFailover** command to further evaluate the attached modems. It is important to wait approximately 5 minutes after a failover (or restart) to allow the system to correctly set up the modems.
2. For security reasons, the modem session is disconnected if the modem cable is detached while a session is active.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1306
3690
Doc:

Chapter 6. Installing and removing an additional 2109 Model M12

This chapter describes how to install and remove an additional 2109 Model M12 from a Model C36 cabinet.

Installation considerations and safety guidelines

DANGER

A fully populated 2109 Model M12 weighs approximately 115 kg (250 lbs) and requires a minimum of two people and a lift tool to install it. Before you install it, verify that the additional weight of the chassis does not exceed the cabinet's weight limit or unbalance the cabinet. When you calculate the additional weight, include the cards or power supplies that partially extend out of the chassis.

Attention: To ensure adequate cooling, install the chassis with the port side facing the aisle where exhaust air is released (usually called the service aisle). This prevents the fans from pulling in heated exhaust air.

Before you install an additional 2109 Model M12 into the cabinet, perform the following tasks:

- Ensure that a space that is 14U high, 74 cm (29 in.) deep, and 48 cm (19 in.) wide is available in the cabinet.
- Ensure that there is a minimum distance of 71.75 cm (28.25 in.) between the front and back rails of the cabinet.
- Verify that the additional weight of the chassis does not exceed the weight limit of the cabinet.
- Ensure that all equipment that is installed in the cabinet is grounded through a reliable branch circuit connection. Do not rely on a secondary connection to a branch circuit, such as a power strip.
- Plan for managing the cables before you install the chassis. You can manage the cables in a variety of ways, such as:
  - Routing the cables below the chassis
  - Routing the cables to either side of the chassis
  - Routing the cables through the cable channels on the sides of the cabinet
  - Using the patch panels
- Ensure that the power directors have two dedicated electrical branch circuits with the following characteristics available for use:
  - 200 - 240 V ac, 30 amps
  - 50 - 60 Hz
- Ensure that the two dedicated electrical branch circuits are protected with a circuit breaker that is in accordance with the local electrical codes.
- Ensure that the supply circuit, line fusing, and wire size are adequate according to the electrical rating on the chassis nameplate.
- Ensure that a licensed electrician installs the grounded outlets and that they are compatible with the power cords.

ECT 1307 3690
CPMI - CORREIOS
Fls. Nº 1307
Doc: 3690

© Copyright IBM Corp. 2002, 2003

- Ensure that the 2109 Model M12 has access to a minimum airflow of 350 cubic feet per minute.
- Ensure that the air temperature that is measured at the blower inlet does not exceed 40°C (104°F) during operation.

Ordering the lift tool

The ordering procedures are different for the lift tool and depend on your location. You should direct questions about these procedures to your regional specialist.

Note: The bridge tool (PN 18P5855), which is required for installation, is shipped with a new or a replacement 2109 Model M12. The bridge tool, when installed, serves as a temporary ramp between the lift tool and the 2109 Model M12 rails that are installed in a Model C36 cabinet. You do not need to return the bridge tool when you are done with it.

World trade locations

The following ordering procedures are for world trade locations:

- Order the lift tool by using the parts order system, like any other part.
- Use the following part numbers when you order:
  - Lift tool: PN 09P2481
  - 24-inch load plate: PN 11P4369
- You do not record parts usage.
- Return the lift tool and the 24-inch load plate to the parts center after you complete the installation or removal of the 2109 Model M12.

United States locations

In the United States, call UPS Logistics at 800-528-6046 to order the lift tool and the 24-inch load plate.

Note: For the SSR branch and territory, the United States cannot order the lift tool or 24-inch load plate through the parts order system. UPS Logistics are used to ship and return the lift tool and 24-inch load plate.

Use the following part numbers when you order:

- Lift tool: PN 09P2481
- 24-inch load plate: PN 11P4369

Note: When you order the lift tool, you will receive an 18-inch load plate. Do not use the 18-inch load plate. You must order and use a 24-inch load plate when you install the 2109 Model M12.

You must provide the following information when you order the lift tool. This information is necessary to ensure that the lift tool is delivered when you need it. Failure to provide this information might delay the completion of the order request and the shipping request. It might also result in a time and date to return the tool that is different from what you need.

- Phone number and customer contact
- Account code: 98577
- Time and date of delivery
- Accurate destination address with zip code
- Time and date of return pickup

You must return the lift tool at the time that was scheduled with UPS Logistics. If you need to change the scheduled return time or date, contact UPS Logistics.

You are responsible for ensuring that all of the paperwork and components are packed and restored in the arbocrate (shipping container) of the lift tool. Ensure that the tool is functioning properly before you release the tool to UPS Logistics for return. You are accountable for the tool until UPS Logistics picks up the lift tool for return delivery to their parts storage facility.

Contact your branch office tools coordinator or your region specialist if you have any questions or concerns.

2109 Model M12 standard shipment

A 2109 Model M12 is shipped with the following items:

- The 2109 Model M12, which includes:
  - Four to eight 16-port cards (customer-specified configuration)
  - Two CP cards
  - Four power supplies
  - Three blower assemblies
- One accessory kit that contains the following items:
  - *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*
  - 2109 Model M12 documentation CD-ROM
  - ESD grounding strap
  - One 3.05 m (10 ft) RS-232 serial cable with an RJ-45 style adapter on the end of the cable
  - The 14U chassis mount kit with installation instructions
  - Bridge tool: PN 18P5855

Note: You can order SFP transceivers separately from IBM. The 2109 Model M12 supports both SWL and LWL transceivers.

Unpacking the 2109 Model M12

Perform the following steps to unpack the 2109 Model M12.

Note: This procedure requires a 1/2-in. socket wrench to remove the pallet bolts.

1. Remove the upper portion of the packing crate while the switch is still in the shipping area to reduce clutter at the installation site.
   a. Open the latches that hold the top of the crate to the pallet. To open a latch, pull the handle out, turn it to the left, then slide the latch open.
   b. Lift the top of the crate off the pallet.
   c. Leave the foam on top of the chassis to hold the kits in place during transportation to the installation area.
   d. Do not move the chassis off the pallet until the door is removed.
2. Open the shipping crate by pulling the handle of the latch and turning it counterclockwise. Slide the latch open.
3. Remove the packing foam, antistatic plastic, 14U chassis mount kit, and accessory kit.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1308
Doc: 3690

4. Unscrew the four bolts that hold the 2109 Model M12 to the pallet. See Figure 32. Remove the brackets.

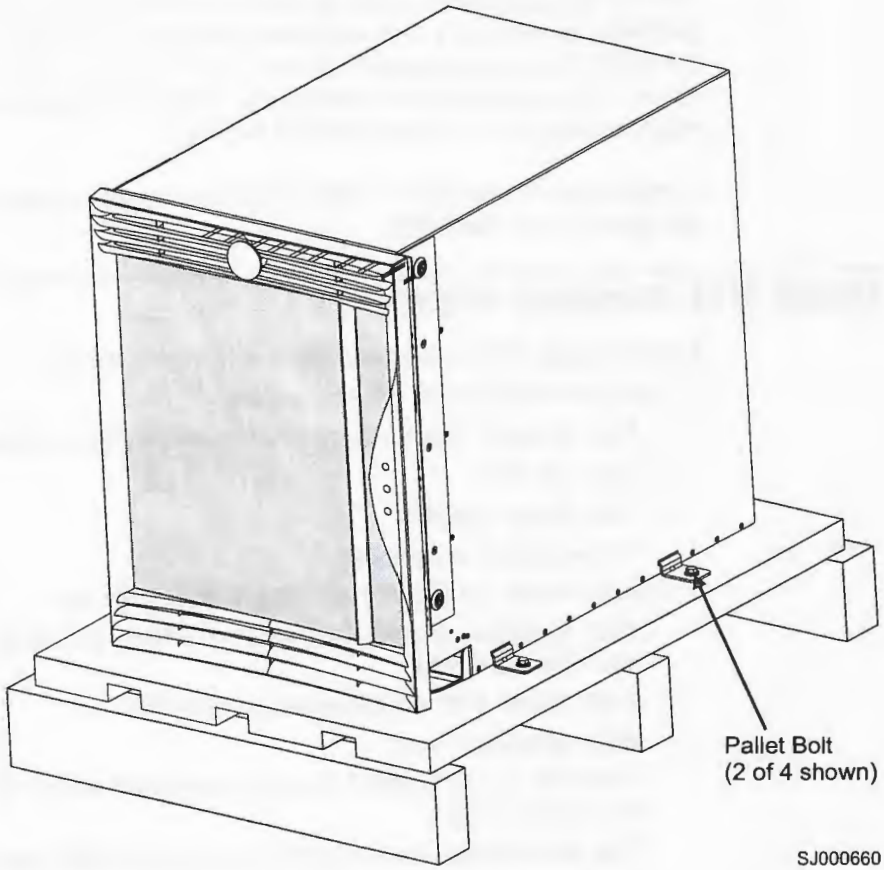


Figure 32. 2109 Model M12 on a pallet

Attention: Remove the chassis door before you move the chassis.

5. Remove the chassis door from the chassis.
   a. Open the door 90°.
   b. Support the door to prevent it from falling. Pull the door away from the chassis.
   c. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge. See Figure 33 on page 55.
   d. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge. Pull the door out, towards you.
   e. Pull the door away from the chassis.

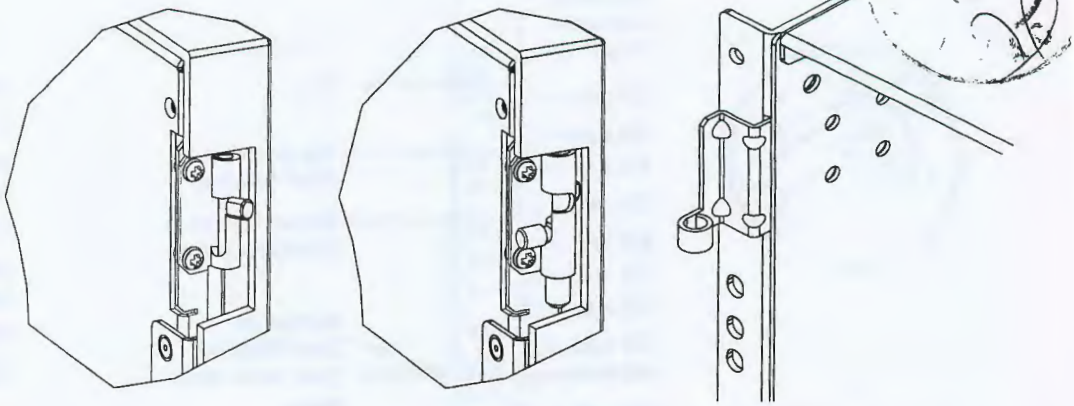


Figure 33. Removing the chassis door

Installing the 2109 Model M12 in the cabinet

This section describes how to install the 2109 Model M12 in the Model C36 cabinet. These procedures use parts that are included in the 14U chassis mount kit. See Table 23 on page 115 for a list of these parts.

Time required

Allow approximately 2.5 hours to complete this procedure. This includes unpacking, assembling, and repacking the lift tool.

Note: Assembly instructions for the lift tool are in the shipping container.

Tools required

You will require the following items to install the 2109 Model M12 in the cabinet:

- #2 Phillips screwdriver
- Lift tool

Installing the brackets

Perform the following steps to install the brackets:

1. Loosen the adjusting screws on the left and right mount shelf brackets to allow for adjustment to the cabinet depth.
2. Attach the left and right mount shelf brackets to the rails in the cabinet. Standard EIA rail spacing of holes is sets of three, separated by 5/8 in., 5/8 in., and 1/2 in. See Figure 34 on page 56.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1309
Doc: 3690

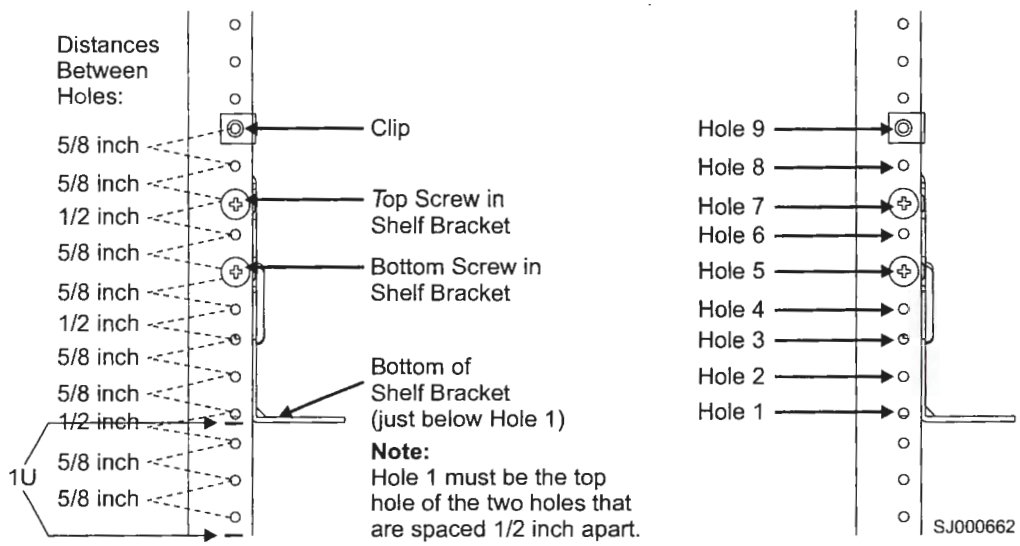


Figure 34. Placement of the shelf brackets and clip nuts on the cabinet rails

Note: If you are installing a 2109 Model M12 into the bottom of the rack, go to step 2a for the location of the rail. If you are installing a 2109 Model M12 into the top of the rack, go to step 2b for the location of the rail.

a. Locate the screws in the middle of EIA unit 5 and the bottom of EIA unit 6 for the back of the cabinet. Locate the screws in the middle of EIA unit 4, the bottom of EIA unit 5, the middle of EIA unit 5, and the bottom of EIA unit 6 for the front of the cabinet.

b. Locate the screws in the middle of EIA unit 22 and the bottom of EIA unit 23 for the back of the cabinet. Locate the screws in the middle of EIA unit 21, the bottom of EIA unit 22, the middle of EIA unit 23, and the bottom of EIA unit 23 for the front of the cabinet.

c. You can route the cables down through the cable management tray or through the holes in the sides of the chassis. If you route the cables down through the cable management tray, allow adequate space below the chassis for cable management.

Orient the left and right mount shelf brackets with the notched portion toward the service aisle. Attach the shelf brackets to the cabinet rails, by using six 1/4-20 x 1/2-in. Phillips panhead screws with lock washers per bracket. Tighten the screws. See Figure 35 on page 57.

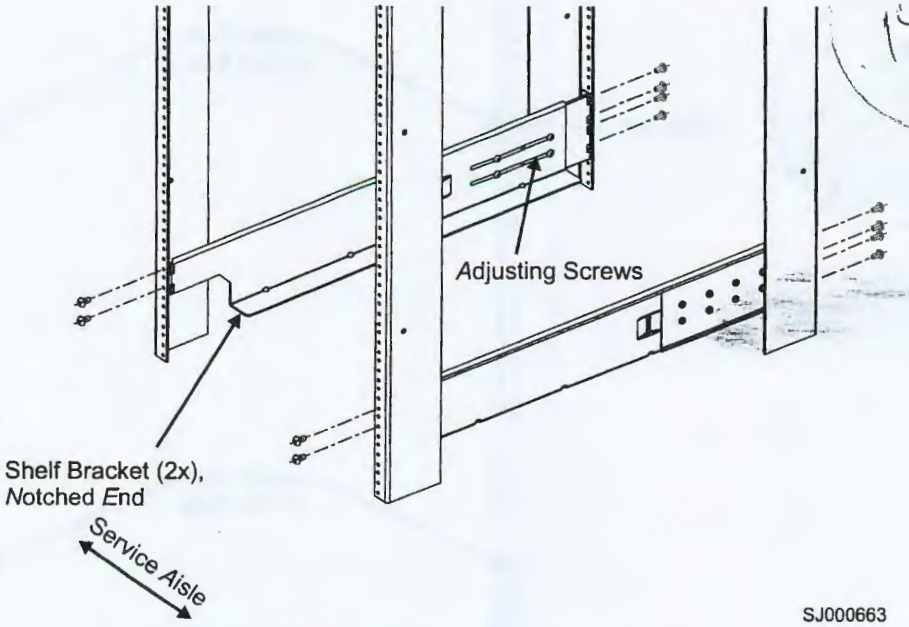


Figure 35. Shelf brackets are installed on the rails (cabinet walls are not shown)

3. Tighten the adjusting screws on the shelf brackets.
4. Attach four 10-32 clip nuts to the two rails at the front of the cabinet (service aisle side). See Figure 36 on page 58.

Note: If you are installing a 2109 Model M12 into the bottom of the rack, go to step 4a for the location of the clip. If you are installing a 2109 Model M12 into the top of the rack, go to step 4b for the location of the clip.

a. Attach the lower clip nuts to the top of EIA unit 6. Attach the upper clip nuts to the middle of EIA unit 17.

b. Attach the lower clip nuts to the top of EIA unit 23. Attach the upper clip nuts to the middle of EIA unit 34.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1310
Doc: 3690

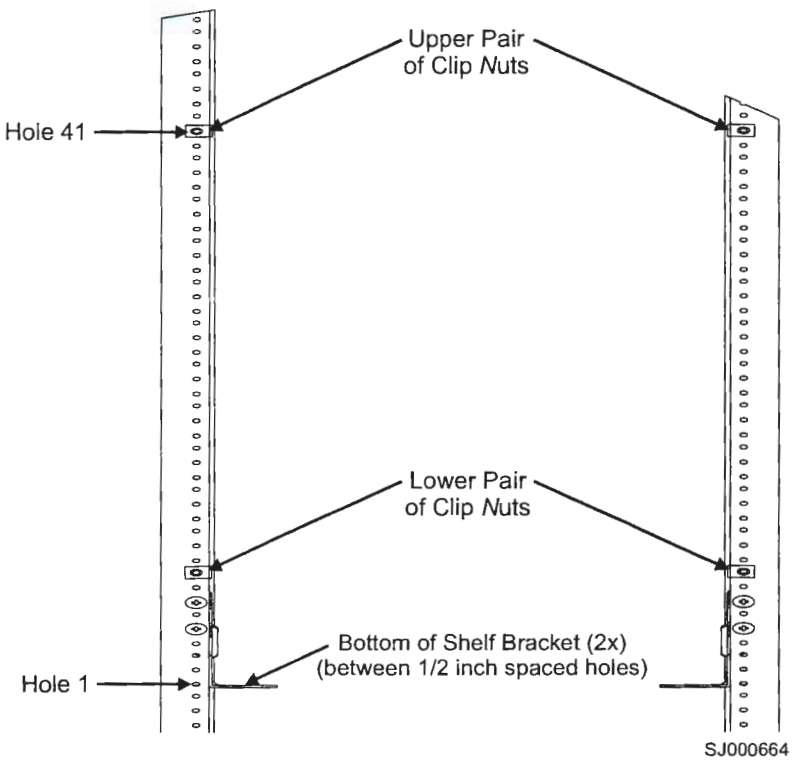


Figure 36. Placing the clip nuts on the rear rails (service aisle side)

5. Disassemble the left and right upper mount bracket assemblies. Save the screws for later use.
6. **Attention:** When you insert screws into the chassis, use the exact screws specified in the procedure. Use of longer screws might damage the chassis.

   Attach the right and left flat upper mount brackets (see Figure 37 on page 59, items 3a and 4a) to the chassis by using four of the 10-32 x 5/16-in. Phillips-flathead screws (item 5) per bracket. Tighten the screws. Orient the slotted holes in the brackets towards the blower side of the chassis. See Figure 37 on page 59 for orientation.

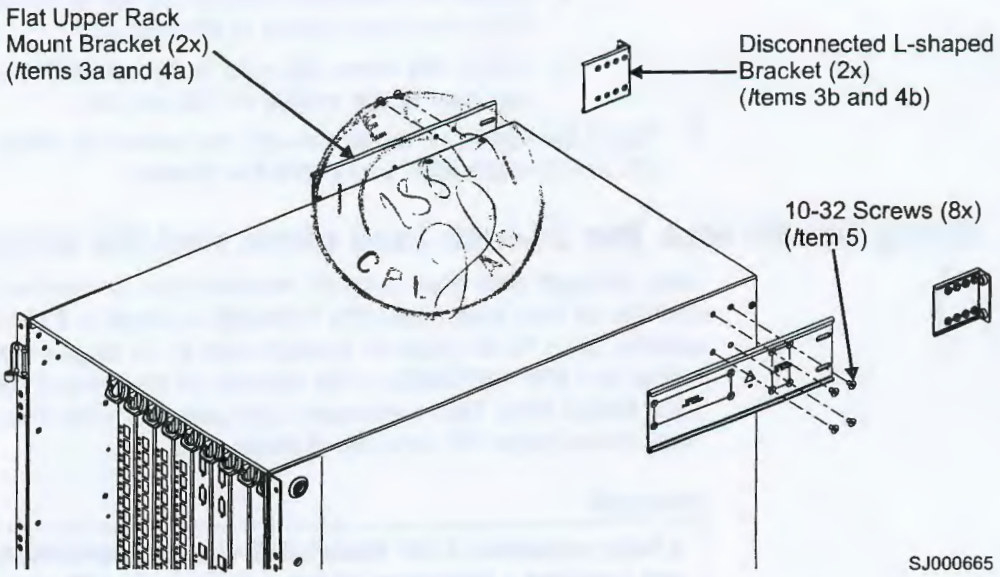


Figure 37. Attaching the right and left flat upper mount brackets to the chassis

7. Attach the two L-shaped upper mount brackets (items 3b and 4b) to the cabinet rails. See Figure 38 for orientation. Use two of the 1/4-20 x 1/2 in. Phillips panhead screws with lock washers per bracket. Tighten the screws.

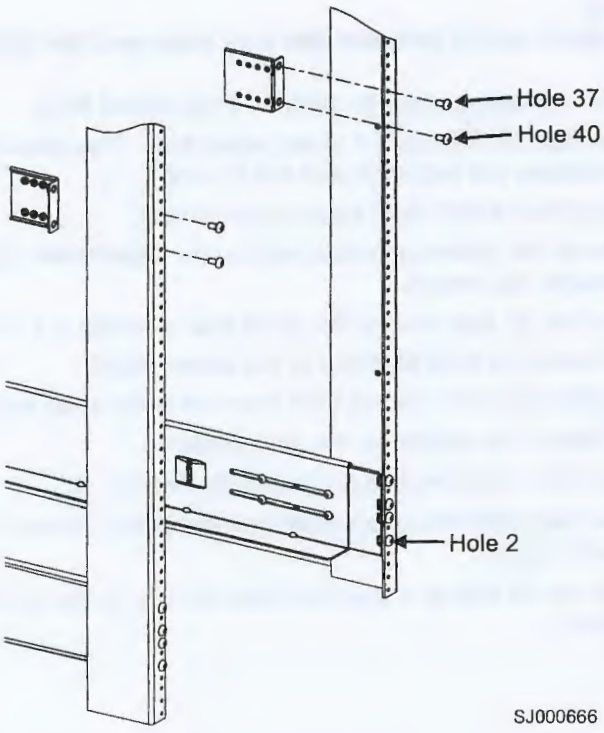


Figure 38. Attaching the L-shaped upper mount brackets to the rails

Note: If you are installing a 2109 Model M12 into the bottom of the rack, go to step 7a on page 60 for the location of the bracket. If you are installing a 2109 Model M12 into the top of the rack, go to step 7b on page 60 for the location of the bracket.

REGISTRO 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1911
Doc: 3690

a. Attach the lower clip nuts to the top of EIA unit 6. Attach the upper clip nuts to the middle of EIA unit 17.
b. Attach the lower clip nuts to the top of EIA unit 23. Attach the upper clip nuts to the middle of EIA unit 34.

8. Route the cables or cords through the cabinet or along any other route that is difficult to reach after you install the chassis.

Using the lift tool, the 24-inch load plate, and the bridge tool

Step 1through step 9 on page 61 describe how to use the lift tool (PN 09P2481) and the 24-inch load plate (PN 11P4369) to install a 2109 Model M12 in the cabinet. Step 10 on page 61 through step 21 on page 64 describe how to install the bridge tool (PN 18P5855) in the cabinet for the lower 2109 Model M12 or the upper 2109 Model M12. This procedure uses parts from the 14U chassis mount kit. See Table 23 on page 115 for a list of these parts.

DANGER

A fully populated 2109 Model M12 weighs approximately 115 kg (250 lbs) and requires a minimum of two people and a lift tool to install it. Before you install it, verify that the additional weight of the chassis does not exceed the cabinet's weight limits or unbalance the cabinet. When you calculate the additional weight, include the cards or power supplies that partially extend out of the chassis.

CAUTION:
A pinch point exists between the load plate and the bridge tool.

Perform the following steps to install a 2109 Model M12:

1. Assemble the lift tool if it is not assembled. The assembly and disassembly instructions are included with the lift tool.
2. Attach the 24-inch load plate to the lift tool.
3. Remove the power supplies and blower assemblies from the 2109 Model M12 to reduce the weight.
4. Move the lift tool next to the pallet that contains the 2109 Model M12.
   a. Adjust the load platform to the same height.
   b. Slide the 2109 Model M12 from the pallet onto the load platform.
   c. Center the switch on the load platform.
5. Attach the retention straps around the drawer.
6. If the load platform is not at its lowest position, lower the load platform to its lowest position.
7. Move the lift tool to a position near the rear of the cabinet. See Figure 39 on page 61.

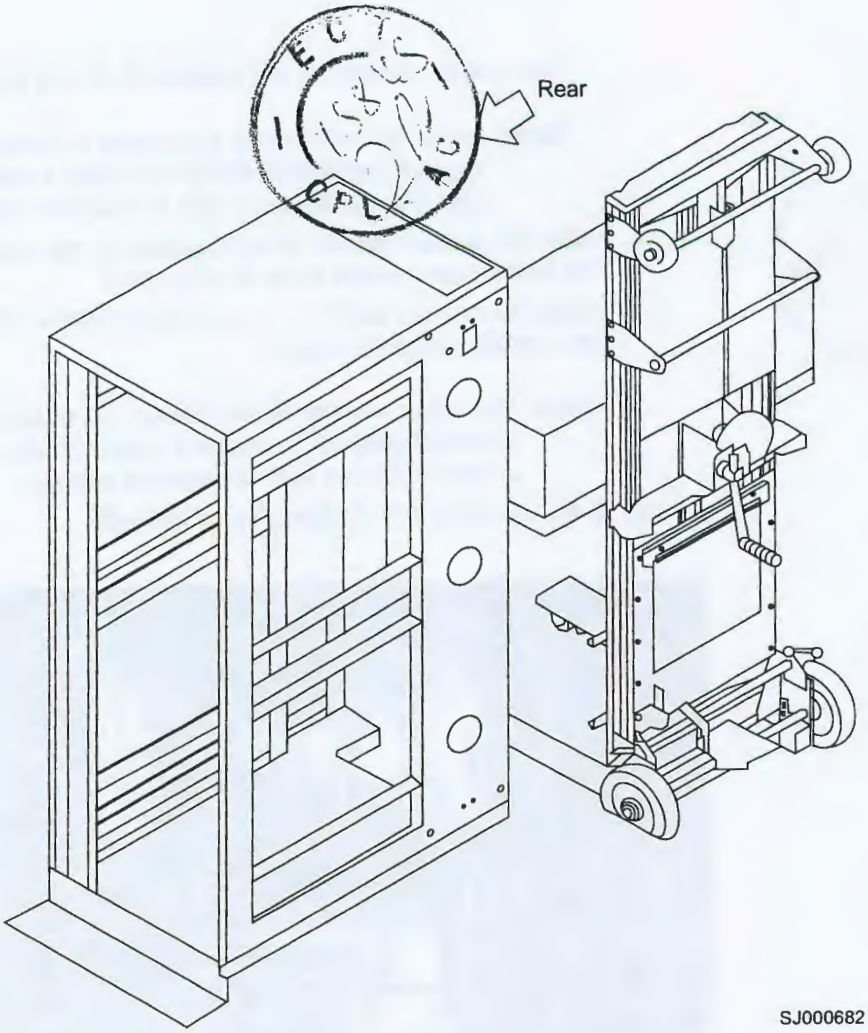


Figure 39. Rear view of cabinet and lift tool

Note: If you are passing through a narrow passage or door, it might be necessary to rotate the drawer on the load platform.

8. Set the wheel brake by pressing down on the wheel brake pedal.
9. Locate the anti-tips bars. If they are not attached, attach them to the lift tool by performing step 9a through step 9d. If the anti-tip bars were previously attached, go to step 10.
   a. Pull up on the leg lock pins and insert the anti-tip bars inside the legs.
   b. Pull on the legs and anti-tip bars to ensure that they are locked into position.
   c. Raise the platform to allow enough room to attach the anti-tip bracket.
   d. Secure the anti-tip bars by using the anti-tip bracket and bolt.
10. If you are installing the lower 2109 Model M12, go to step 11. If you are installing the upper 2109 Model M12, go to step 12 on page 62.
11. For the lower 2109 Model M12, install the bridge tool by completing the following steps:
    a. Remove the bridge tool from the box and adjust the two supports 45°.
    b. Hold the bridge tool between the two vertical supports near EIA unit 3, and move the two supports another 45°. Make sure that the following conditions are met:
       - The two-pin section of the support is on the back of the vertical support.

ROS nº 03/2005 - CN - CPMI - CORREIOS 1312 Fls. Nº 3690

- The one-pin section of the support is on the front of the vertical support.

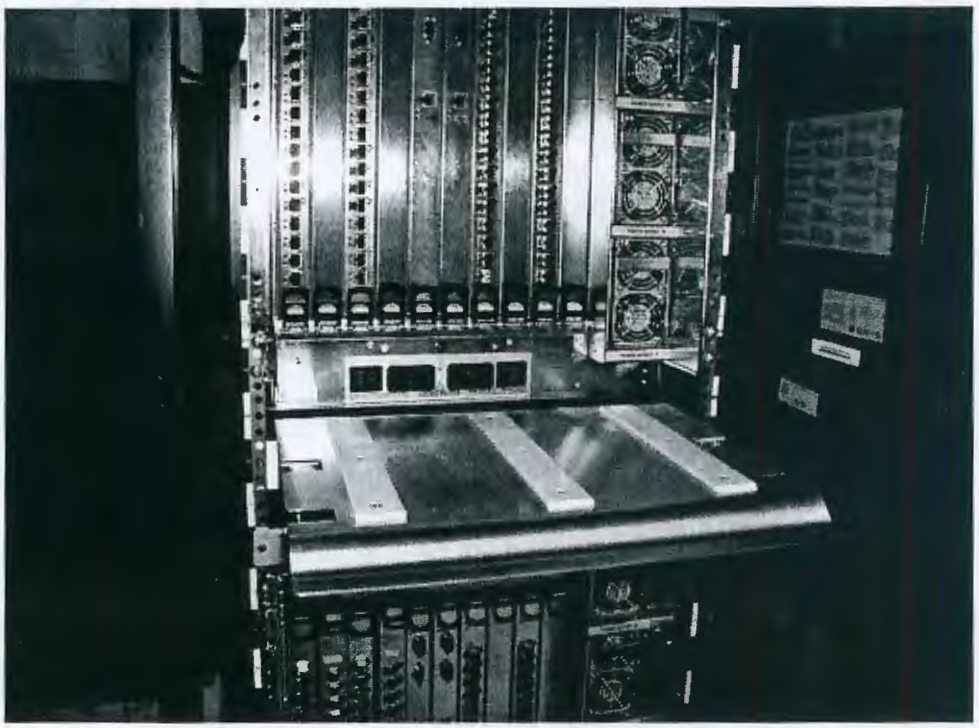
Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and one-pin sections with the vertical support.

c. Align the two-pin section of the support on the back of the vertical rail with the bottom and middle holes in EIA unit 3.

d. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 1.

Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and the one-pin sections with the vertical support.

e. Lock the shelf into position. See Figure 40.



SJ000680

Figure 40. Locking the shelf into position

12. For the upper 2109 Model M12, install the bridge tool by completing the following steps:
    a. Remove the bridge tool from the box and adjust the two supports 45°.
    b. Hold the bridge tool between the two vertical supports near EIA unit 20, and move the two supports another 45°. Make sure that the following conditions are met:
        - The two-pin section of the support is on the back of the vertical support.
        - The one-pin section is on the front of the vertical support.

Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and one-pin sections with the vertical support.

c. Align the two-pin section of the support on the front of the vertical rail with the bottom hole and the middle hole in EIA unit 20.

d. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 18.

13. Turn the winch crank counterclockwise, 1/4 turn, to set the winch brake.
14. Set the wheel brake and place the wheel chocks around the wheels.
15. Remove the retention straps.
16. Slide the switch into the cabinet.
17. Remove the wheel chocks, release the wheel brake, and move the lift tool away from the cabinet.
18. Reinstall the power supplies and blower assemblies.
19. Fasten the two flat left and right upper mount brackets that are on the chassis to the two L-shaped upper left and right cabinet mount brackets. Use the two screws that were set aside in step 5 on page 58. Tighten the screws. See Figure 41.

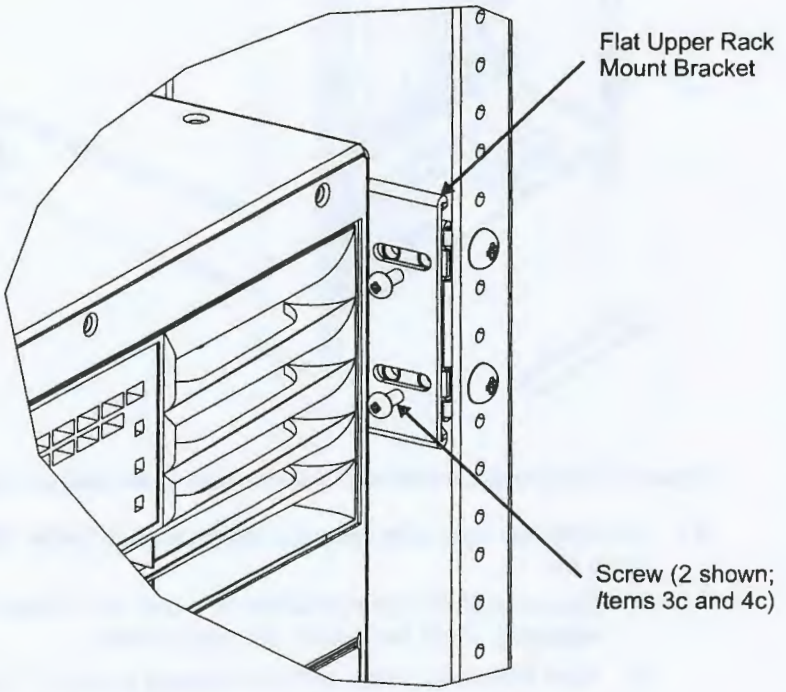


Figure 41. Attaching the mount brackets to the cabinet rails

20. Fasten the port side of the chassis to the cabinet rails. Use two of the 10-32 x 5/8-in. Phillips panhead screws with washers on each side. Tighten the screws. See Figure 42 on page 64 for the location of the screws.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 1313
Doc: 3690

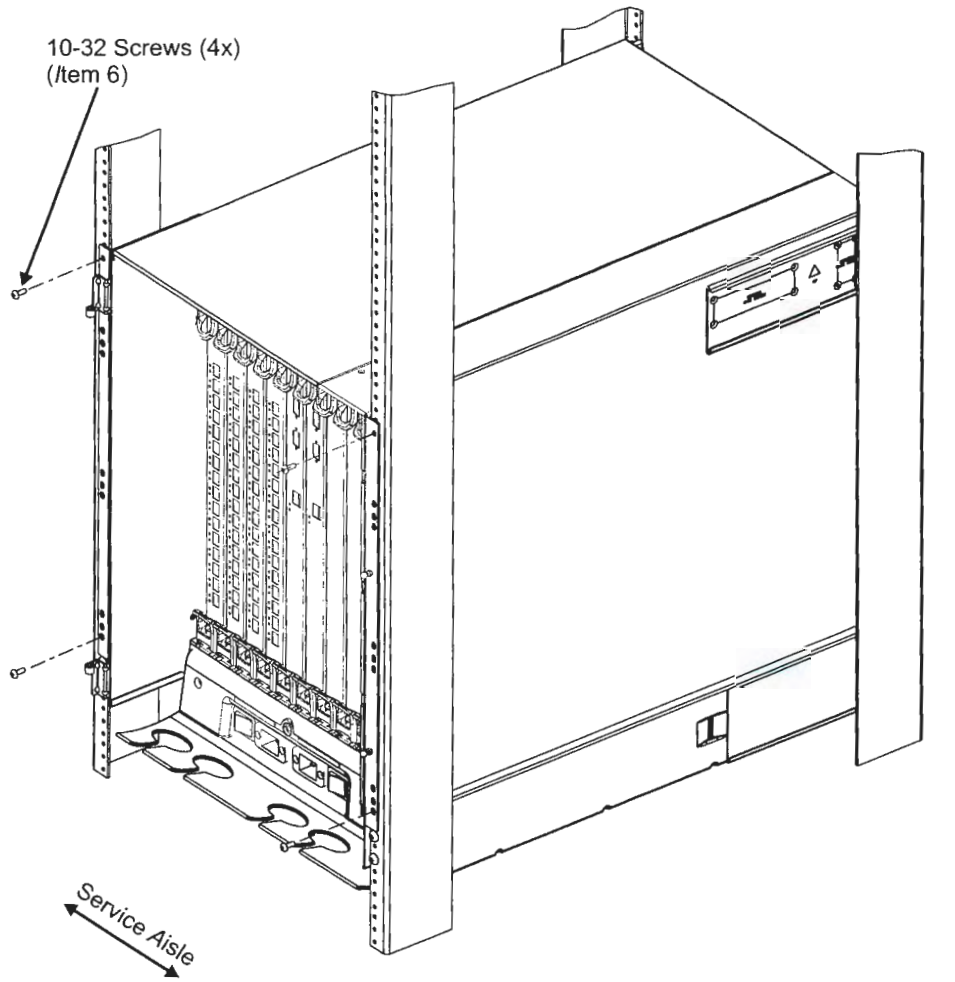
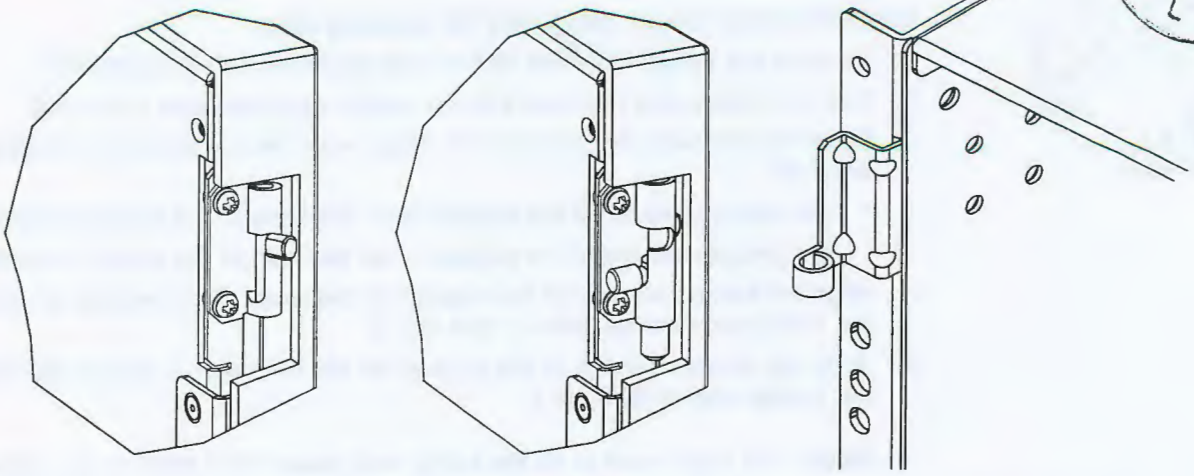


Figure 42. Attaching the port side of the chassis to the cabinet rails

21. Reinstall the door after you put the chassis in place. See Figure 43 on page 65.
    a. Ensure that the spring-loaded pins that are on both door hinges are retracted. Push the levers into the notches.
    b. Align the door hinges with the chassis portion of the hinges.
    c. Release the pins by pushing the levers out of the notches.



Upper Door Hinge with Lever in *N*otch

Upper Door Hinge with Lever *O*ut of *N*otch (Pin Released)

Chassis Portion of Hinge

SJ000661

Figure 43. Removing the chassis door

22. Uninstall the bridge tool and return it to its original box.

Note: For turning on the power and for the configuration instructions, see Chapter 3, "Starting and configuring the 2109 Model M12", on page 19.

Attention: Do not connect the switch to the network until the IP addresses are correctly set.

Removing a 2109 Model M12 from the cabinet

Step 1 through step 5 describe how to use the lift tool (PN 09P2481) and the 24-inch load plate (PN 11P4369) to remove a 2109 Model M12 from the cabinet. Step 6 on page 66 through step 17 on page 67 describe how to remove the bridge tool (PN 18P5855) from the cabinet for the lower 2109 Model M12 or the upper 2109 Model M12.

Perform the following steps to remove a 2109 Model M12:

1. Assemble the lift tool if it is not assembled. The assembly and disassembly instructions are included with the lift tool.
2. Remove both power cords from the 2109 Model M12.
3. Remove the power supplies and blower assemblies from the 2109 Model M12 to reduce the weight.
4. Remove the chassis door from the chassis.
   a. Open the door 90°.
   b. Support the door to prevent it from falling.
   c. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge. See Figure 33 on page 55.
   d. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge. Pull the door out and towards you.
   e. Pull the door away from the chassis.
5. Remove the two 10-32 x 5/8 in. Phillips panhead screws with washers on each side. See Figure 41 on page 63 for the location of the screws.

RQS nº 03/2005 - CN - CRM/ CORREIOS
Fls. Nº 1314
Doc: 3690

6. If you are replacing the lower 2109 M12, go to step 7. If you are replacing the upper 2109 M12, go to step 8.
7. Install the bridge tool by completing the following steps:
   a. Remove the bridge tool from its box and adjust the two supports 45°.
   b. Hold the bridge tool between the two vertical supports near EIA unit 3.
   c. Move the two supports another 45°. Make sure that the following conditions are met:
      - The two-pin section of the support is on the back of the vertical support
      - The one-pin section of the support is on the front of the vertical support
   d. Align the two-pin section of the support on the back of the vertical rail with the bottom and middle holes in EIA unit 3.
   e. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 1.

      Note: You might want to tilt the bridge tool towards the back of the cabinet approximately 45° to make it easier to align the two-pin and one-pin sections with the vertical support.

   f. Lock the shelf into position.
8. For the upper 2109 Model M12, install the bridge tool by completing the following steps:
   a. Remove the bridge tool from its box and adjust the two supports 45°.
   b. Hold the bridge tool between the two vertical supports near EIA unit 20.
   c. Move the two supports another 45°. Make sure that the following conditions are met:
      - The two-pin section of the support is on the back of the vertical support
      - The one-pin section of the support is on the front of the vertical support
   d. Align the two-pin section of the support on the back of the vertical rail with the bottom and middle holes in EIA unit 20.
   e. Align the one-pin section of the support on the front of the vertical rail with the middle hole in EIA unit 18.
   f. Lock the shelf into position.
9. Locate the anti-tip bars and if they are not attached, attach them to the lift tool. If anti-tip bars were previously attached, go to step 10.
   a. Pull up on the leg-lock pins and insert the anti-tip bars inside the legs.
   b. Pull on the legs and anti-tip bars to ensure that they are locked into position.
   c. Raise the platform to allow enough room to attach the anti-tip bracket.
   d. Secure the anti-tip bars with the anti-tip bracket and bolt.
10. Move the lift tool to a position near the rear of the cabinet.
11. Turn the winch crank clockwise to raise the switch. Move the lift tool into position in front of the cabinet while you align the 24-inch load plate with the line on the bridge tool.
12. Turn the winch crank counterclockwise 1/4 turn to set the winch brake.
13. Set the wheel brake. Place the wheel chocks around the wheels.

DANGER

A fully populated 2109 Model M12 weighs approximately 115 kg (250 lbs) and requires a minimum of two people and a lift tool to install it. Before you install it, verify that the additional weight of the chassis does not exceed the cabinet's weight limits or unbalance the cabinet. When you calculate the additional weight, include the cards or power supplies that partially extend out of the chassis.

CAUTION:
A pinch point exists between the 24-inch load plate and the bridge tool.

14. Slide the switch from the cabinet onto the 24-inch load plate. Center the switch on the platform.
15. Install the retention straps.
16. Remove the wheel chocks, release the wheel brake, and move the lift tool away from the cabinet.
17. Lower the load platform to its lowest position.
18. Remove the bridge tool.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1315
3690
Doc:

Chapter 7. Servicing the 2109 Model C36 with Model M12

This chapter contains information about how to power on and off the cabinet, and remove and replace FRUs and other system components.

Safety notices

The following safety notices apply to all the procedures in this chapter. Review this section carefully before you perform any power-related operations.

DANGER

An incorrectly wired electrical outlet could place hazardous voltage on metal parts of the system or the devices that attach to the system. The customer is responsible to ensure that the outlet is correctly wired and grounded to prevent an electrical shock.

Before you install or remove signal cables, ensure that you have unplugged the power cables for the system unit and all attached devices.

When you add or remove any additional devices to or from the system, ensure that you unplugged the power cables for those devices before you connect the signal cables. If possible, disconnect all power cables from the existing system before you add a device.

Use one hand, when possible, to connect or disconnect signal cables to prevent a possible shock from touching two surfaces with different electrical potentials.

During an electrical storm, do not connect cables for display stations, printers, telephones, or station protectors for communication lines.

CAUTION:
This unit might have more than one power cable. To completely remove power, you must disconnect all power cables from the unit.

CAUTION:
"Norway only:" This product is designed for an IT power system with phase-to-phase voltage of 230V. After operation of the protective device, the equipment is still under voltage if it is connected to an IT power system.

Power-on procedure

Perform the following steps to power on the cabinet:

1. Plug all power cords into the outlets on the power distribution units (PDUs).
2. Plug the power cord of each PDU into the customer's ac power outlets.

   CAUTION:
   This product is equipped with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded electrical outlet to avoid electrical shock.
3. Follow the power-on procedures for the 2109 Model M12 that is installed in the cabinet. See "Turning on and off the 2109 Model M12" on page 27.
4. Close the front door of the cabinet.

© Copyright IBM Corp. 2002, 2003

CPMI - CORREIOS
1316
Fls. Nº
Doc: 3690

Power-off procedure

Perform the following steps to power off the cabinet:

1. Open the rear door of the cabinet.

   Check the power cabling from the 2109 Model M12 that is attached to the PDU that you are servicing. These switches have dual power cords and are plugged into PDUs with independent ac sources.
2. Removing power to a mounted 2109 Model M12 has an adverse affect on the customer's systems and networks if they are not properly prepared. Inform the customer before you power off the 2109 Model M12.

   Before you power off switches, make sure that the customer has removed, dismounted, or taken them offline from their systems.
3. Turn off the ac power switches (circuit breaker) to the 2109 Model M12 that are connected to the PDU that you are servicing.
4. Unplug the power cord from the customer's ac power outlet.
5. Unplug all power cords from the PDU that you are servicing.

Removing and replacing a 16-port card or filler panel

Use this procedure to remove and replace a 16-port card or filler panel. The 2109 Model M12 can continue to operate during this procedure. However, if you are removing a 16-port card, any cables that are connected to that 16-port card must be disconnected.

You can notify the 2109 Model M12 of a hot-swap request in two ways. You can either run the **slotPowerOff** and **slotPowerOn** commands, or click the ejector handles on the 16-port card.

Attention: Do not remove the 16-port card during diagnostic tests. Wait for the status LED to turn off in response to the hot-swap request before you remove a 16-port card.

Attention: Disassembling any part of a 16-port card or filler panel voids the part warranty and regulatory certifications.

Attention: To ensure correct cooling of the chassis and protection from dust, install a filler panel in any empty slots.

CAUTION:
No user-serviceable parts are inside the 16-port card or filler panel.

Time required

Approximately 10 minutes or less

Removing a 16-port card or filler panel

Attention: Wear a grounded ESD strap when handling a 16-port card. The chassis has a grounding connection above the power connectors. Hold the 16-port card by the edges of the metal pan (do not hold by ejectors).

Note: If you are replacing multiple cards, replace one card at a time. Before you replace a port card, determine if it is the entire card or the SFPs that are faulty.

Perform the following steps to remove a 16-port card:

1. Ensure that traffic is not flowing through the port card (port LEDs should be off) before you disconnect the cables.
2. Disconnect any cables and SFP transceivers from the port card.
3. Notify the switch of a hot-swap request by pushing in the yellow tab on each ejector and clicking the black handles slightly open. See Figure 44 on page 72.

   Note: You can also send hot-swap notification from the command line interface by using the **slotpoweroff** and **slotpoweron** commands. See the *Brocade Fabric OS Procedures Guide* for additional command line instructions.
4. Wait for the Power LED to turn off in response to the hot-swap request before you uninstall the port card.
5. Lever both ejectors open to approximately 45° and pull the port card out of the chassis.

   Note: If you inadvertently re-latch the ejectors before you remove the card, wait at least one second before you unlatch the ejectors again.
6. If you are not replacing the card by another port card, install a filler panel to ensure correct cooling of the chassis and protection from dust. For more information, see "Replacing a 16-port card or filler panel" on page 74.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1317
Doc: 3690

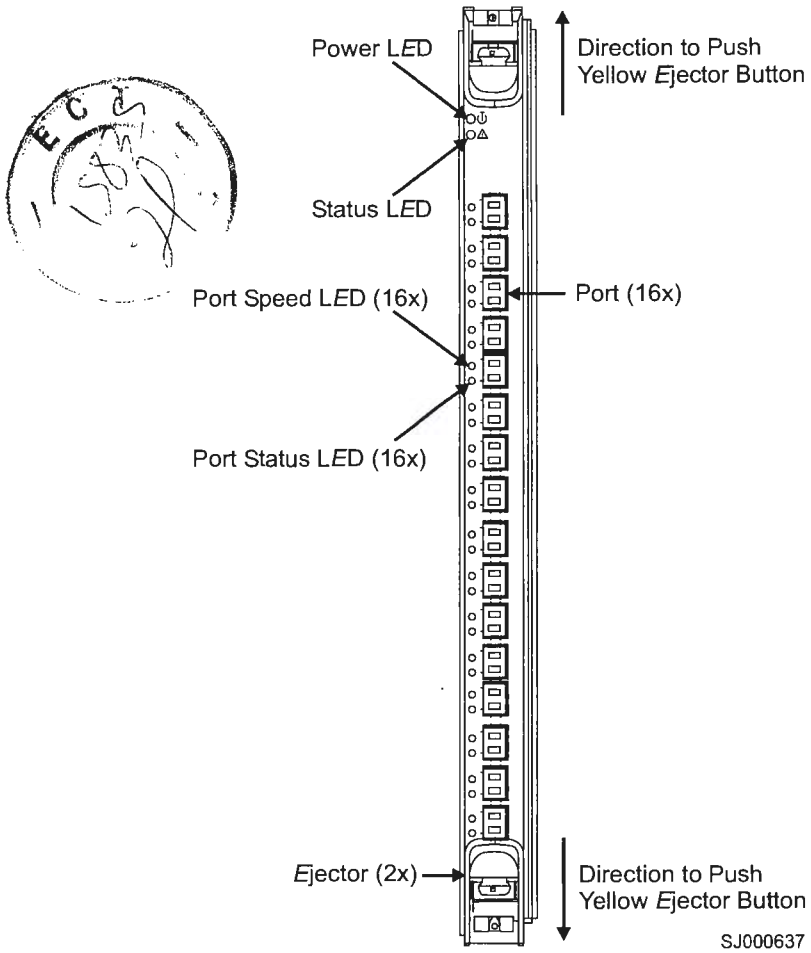


Figure 44. 16-port card showing ejectors

Removing a filler panel

The 2109 Model M12 accommodates the following two types of filler panels:

- A filler panel with ejectors
- A filler panel without ejectors

Perform the following steps to remove a filler panel with ejectors:

1. Push the yellow tab in on each ejector. See Figure 45 on page 73.
2. Lever both ejectors all the way open.
3. Slide the filler panel out of the chassis. See Figure 46 on page 74

Note: Filler panels without ejectors are equipped with a handle. Remove the two captive screws, grasp the handle, and slide the filler panel out.

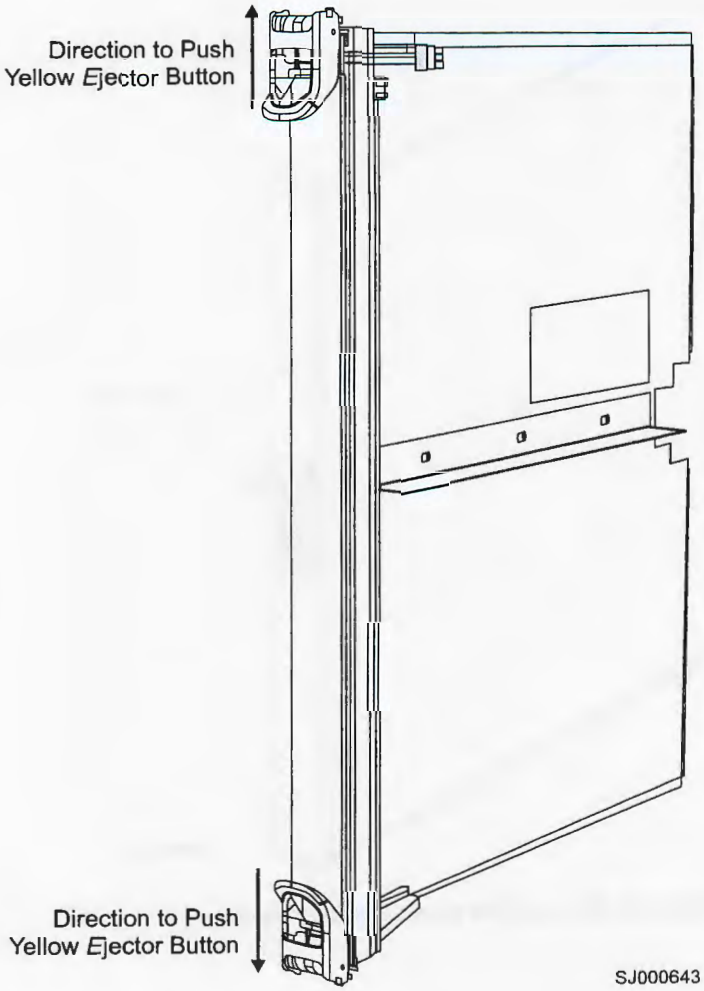


Figure 45. 16-port card filler panel

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1318
Fls. Nº
Doc: 3690

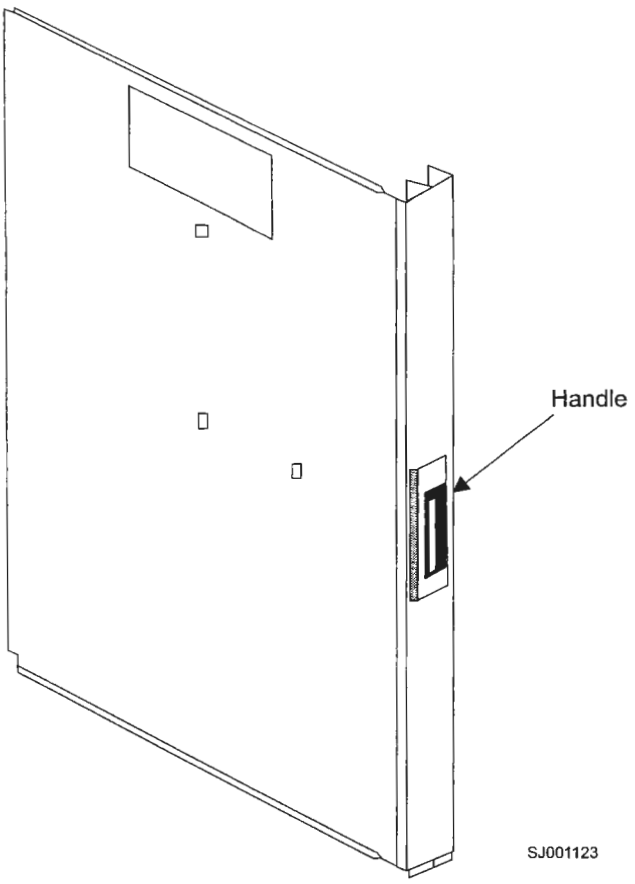


Figure 46. CP card filler panel with one handle

Replacing a 16-port card or filler panel

Attention: Do not force the installation. If the 16-port card or filler panel does not slide in easily, ensure that it is correctly aligned inside the rail guides before you continue.

Perform the following steps to replace a 16-port card or filler panel:

1. Orient the 16-port card or filler panel so that the ejectors are at the front of the chassis and the flat side of the 16-port card or filler panel is on the left.
2. Align the flat side of the 16-port card or filler panel inside the upper rail guides and the lower rail guides in the slot. See Figure 47 on page 75. Slide the 16-port card or filler panel into the slot, with slight pressure to the left, until it is firmly seated.
3. Close the ejectors by rotating the black handles toward the center of the 16-port card or filler panel until the ejectors lock. You will hear a slight audible click. The levering action of the handles seats the 16-port card or filler panel in the slot.

   Figure 47 on page 75 shows the alignment guides in the card slots.

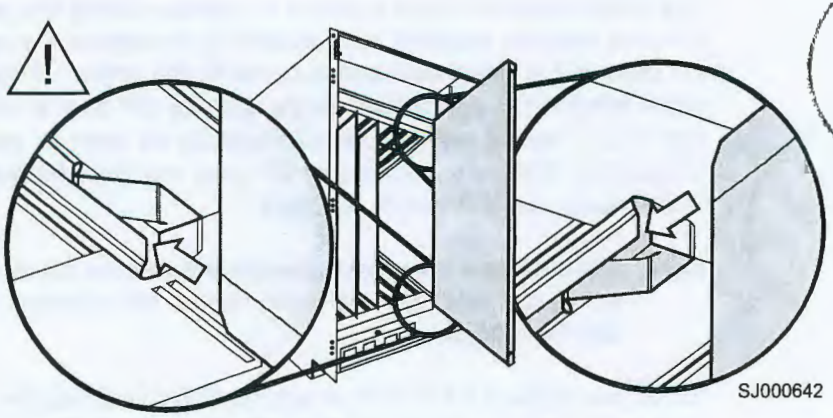


Figure 47. Alignment guides in the card slots

Perform these additional steps if you are installing a new 16-port card:

1. Verify that the power LED on the 16-port card is displaying a steady green light (it might require a few seconds to turn on). If it does not turn on, ensure that the 16-port card has power and is firmly seated. The front of the 16-port card should be flush with any adjacent 16-port cards or filler panels.

   Note: The LED patterns can temporarily change during a POST and other diagnostic tests.
2. Install SFPs and cables in the 16-port card, as required.
3. Group and route the cables as desired. See "Guidelines for managing cables" for more information.

   Attention: Do not route cables in front of the exhaust vent (located at the top of the chassis on the port side).

Guidelines for managing cables

The following guidelines are for managing cables:

- You can manage cables in a variety of ways. You can route them down through the cable management tray or route them out either side of the chassis. You can also manage them by using patch panels or cable channels on the sides of the cabinet.
- To keep the LEDs visible and to prevent having to disconnect the cables when removing neighboring cards, route fiber-optic cables and other cables directly downwards, instead of across adjacent cards or in front of the power supplies.
- Leave at least 1 m (3.28 ft) of slack for each fiber-optic cable, which:
  - Provides room to remove and replace the 16-port card
  - Allows for inadvertent movement of the cabinet
  - Prevents the cables from being bent to less than the minimum bend radius

  The minimum bend radius for a 50-micron cable is 3.05 cm (2 in.) under full tensile load and 3.048 cm (1.2 in.) with no tensile load.
- Use the cable guides that are provided with the 2109 Model M12 to group the cables by trunking ports (groups of four neighboring ports). These guides help to keep individual ports accessible by keeping the cables evenly spaced. They also help to provide clearance when removing a neighboring card.

Removing and replacing a CP card or filler panel

Use this procedure to remove and replace a CP card or filler panel.

ROS 5/03/00 - CN - CPM - CORREIOS
Fls. Nº 1319
Doc: 3690

The 2109 Model M12 can continue to operate during this procedure if at least one CP card remains installed and functioning throughout the procedure. However, if the CP card that is being replaced is currently the active CP card, traffic over the fabric stops temporarily until failover to the standby CP card is complete. Failover takes less than 1 minute and occurs automatically as soon as the active CP card is uninstalled. If there is no standby CP card, the 2109 Model M12 stops functioning until at least one CP card is installed.

Note: The **haShow** command provides information about which CP card is the active CP card. For information about this command, see the *Brocade Fabric OS Reference.*

When you replace a CP card, it automatically assumes the native IP address and host name that is assigned to that slot. The default IP address and host name are `10.77.77.75 CP0`, for slot 5 and `10.77.77.74 CP1` for slot 6.

CAUTION:
Disassembling any part of a CP card or filler panel voids the part warranty and regulatory certifications. No user-serviceable parts are inside a CP card or filler panel. To ensure correct cooling of the chassis and protection from dust, install a filler panel in any slots that do not contain a CP card.

CAUTION:
Do not attempt to replace the RTC (real time clock) battery on the CP card. There is danger of explosion if you incorrectly replace the battery. Contact IBM because you must replace the battery with the same type of battery that the manufacturer recommends. You must also dispose of it according to the manufacturer's instructions.

Attention: Use the same version of Fabric OS on both CP cards and logical switches. Using different versions might cause malfunctioning. If the replacement CP card has a different version of the Fabric OS, bring both cards to the same firmware version.

Time required

30 minutes or less

Items required

- ESD grounding strap
- Workstation computer
- Serial cable provided with the 2109 Model M12
- IP address of an FTP server for backing up the switch configuration

Confirming a failed CP card

Before you replace the CP card, verify the necessity of the replacement. Any of the following events might indicate that a CP card is faulty:

- The Status LED on the CP card is orange, or the Power LED is not lit.
- The **slotshow** command does not show that the CP card is enabled.
- The CP card does not respond to commands or private Ethernet activities, or the serial console is not available.
- The **hashow** command indicates that the CP card has not achieved redundancy.

- The calendar clock is inaccurate, or the CP card does not start or shut down normally.
- Any of the following messages display in the error log:
  - Slot unknown message that relates to a CP slot
  - CP card errors
  - FRU: FRU_FAULTY messages for a CP card
  - Configuration loader messages or Sys PCI config messages
  - Generic system driver messages (FABSYS)
  - Platform system driver messages (Platform)
  - EM messages that indicate a problem with a CP card
  - Function fail messages for the CP master

For more information about diagnostic and error messages, see the *Brocade Diagnostic and System Error Message Reference* and the *Brocade Fabric OS Procedures Guide*.

Recording critical switch information for a CP card

Perform the following steps to record critical switch information:

1. Create a serial connection to the healthy CP card:
   a. Disable any serial communication programs that are running on the workstation (such as synchronization programs).
   b. Insert one of the serial cables into the terminal serial port. See the second port from the top in Figure 48 on page 80.
   c. Connect the other end of the serial cable to a serial port on the workstation. If necessary, you can remove the adapter on the serial cable to allow for a serial RJ45 connection.
   d. Open the terminal emulator application and configure as follows:
      - For most UNIX systems, type the following string at the prompt:
        `tip /dev/ttyb -9600`
      - For Windows 95, 98, 2000, or NT, see the following table for parameters and values.

Table 8. Parameters and values

Parameter	Value
Bits per second	9600
Databits	8
Parity	None
Stop bits	1
Flow control	None

   e. When the terminal emulator application stops reporting information, press Enter.
2. Log into the healthy CP card as `Admin`, then type `0` to log into switch 0. The default password is `password`.

RQS nº 03/2006 - CN -
CPMI - CORREIOS
Fls: Nº 1320
Doc: 3690

See the following example for possible output.

```
Fabric OS (cp0)
cp0 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin>
```

3. Run the **haShow** command to determine which CP card is active. Do this from the serial console for the healthy CP card to verify the failover.

   Note: Enter all the remaining commands from the serial console for the active CP card, unless otherwise indicated.

4. If the healthy CP card is performing as the active CP card, go to step 7. If the faulty CP card is performing as the active CP card, fail over the cards as steps 4a through 4e describe:
   a. Create a serial connection to the faulty CP card (repeat step 1 on page 77.
   b. Log into the serial console as `Admin` and type `0` to log into logical switch 0.
   c. Run the **hafailover** command. The healthy CP card becomes the active CP card.
   d. Wait until the Status LED on the healthy CP card is no longer lit, which indicates that failover is complete.
   e. Run the **hashow** command from the serial console for the healthy CP card to verify the failover.

      See the following example for possible output.

```
Fabric OS (cp1)
cp1 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin> hashow
Local CP (Slot 6, CP1) : Active
Remote CP (Slot 5, CP0) : Standby
HA Enabled, Heartbeat Up
SW0:admin>
SW0:admin> hafailover
Warning: This command is being run on a control processor(CP)
based system and will cause the active CP to reset. This will
cause disruption to devices attached to both switch 0 and switch 1
and will require that existing telnet sessions be restarted.
To just reboot a logical switch on this system, use command
switchreboot(1M) on the logical switch you intend to reboot.
Are you sure you want to reboot the active CP [y/n]? y
SW0:admin>
SW0:admin> hashow
Local CP (Slot 6, CP1) : Standby, Healthy
Remote CP (Slot 5, CP0) : Active
HA Enabled, Heartbeat Up
SW0:admin>
```

5. Run the **version** command to record the version of the active CP card.
6. Run the **hadisable** command from the active CP card to prevent failover or communication between the CP cards during the replacement.
7. From the serial console for the healthy (and active) CP card, back up the current configuration for logical switch 0. See the possible output from the **configupload** command in step 8 on page 79.

a. Run the **configupload** command.
b. Enter the requested information at the prompts.

8. Log into logical switch 1 and back up the current configuration for switch 1.
   a. From the serial console for the healthy CP card, enter the **login** command.
   b. Log into the switch as `Admin` and enter `1` to log into Switch 1.
   c. Enter the **configupload** command.
   d. Enter the requested information at the prompts.
      See the following example for possible output.

```
SW0:admin> configupload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
upload complete
SW0:admin>
SW0:admin> login
cp0 login: admin
Password: xxxxxx
Enter Switch Number to Login <0 or 1>: 1
SW1:admin>
SW1:admin> configupload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
upload complete
SW1:admin>
```

Removing a CP card or filler panel

Attention: Wear an ESD grounding strap when handling a CP card. The chassis has a grounding connection above the power connectors.

Attention: Hold the CP card by the edges of the metal pan (not by the ejectors).

Note: To allow the current configuration to be copied to the new CP card, you must install a new CP card while the other CP card is still operating.

Perform the following steps to remove a CP card:

1. Ensure that the other CP card is healthy and functioning as the active CP. See "Confirming a failed CP card" on page 76 for more information. Run the **haShow** command to determine which is the active CP card.
2. If the card that you are replacing is the standby CP card, continue with step 3. If the card that is being replaced is the active CP card, verify that the standby CP card is healthy. The power LED should be green, and the status LED should not be lit. Run the **haFailover** command to make the standby CP card act as the new active CP card.
3. Remove the CP card that you are replacing.
   a. Disconnect the following cables if they are present:
      - Modem cable from the modem serial port
      - Serial cable from the terminal serial port
      - Ethernet cable from the Ethernet port

RQS nº 03/2005 - CN
CPMI - CORREIO
1321
Fls. Nº
Doc: 3690

b. Notify the switch of a hot-swap request by pushing the yellow tab on each ejector and clicking the black handles until they are slightly open. See Figure 48. Wait for the status LED to turn off.

   Attention: If you are removing a CP card, wait for the status LED to turn off in response to the hot-swap request before you uninstall the card.

c. Lever both ejectors all the way open, and slide the CP card out of the chassis.

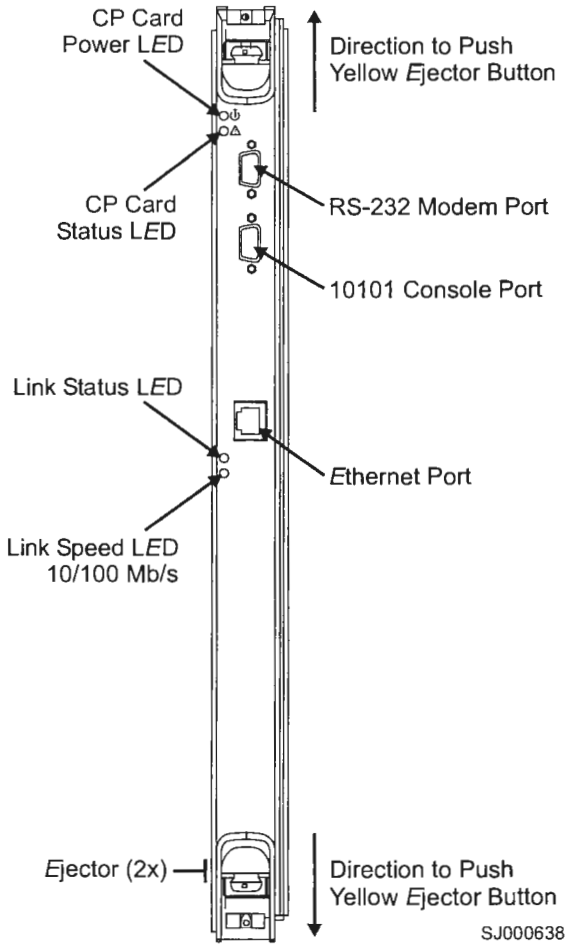


Figure 48. CP card showing ejectors

Perform the following steps to remove a filler panel:

1. Push in the yellow tab on each ejector. See Figure 49 on page 81.
2. Lever both ejectors all the way open.
3. Slide the filler panel out of the chassis.

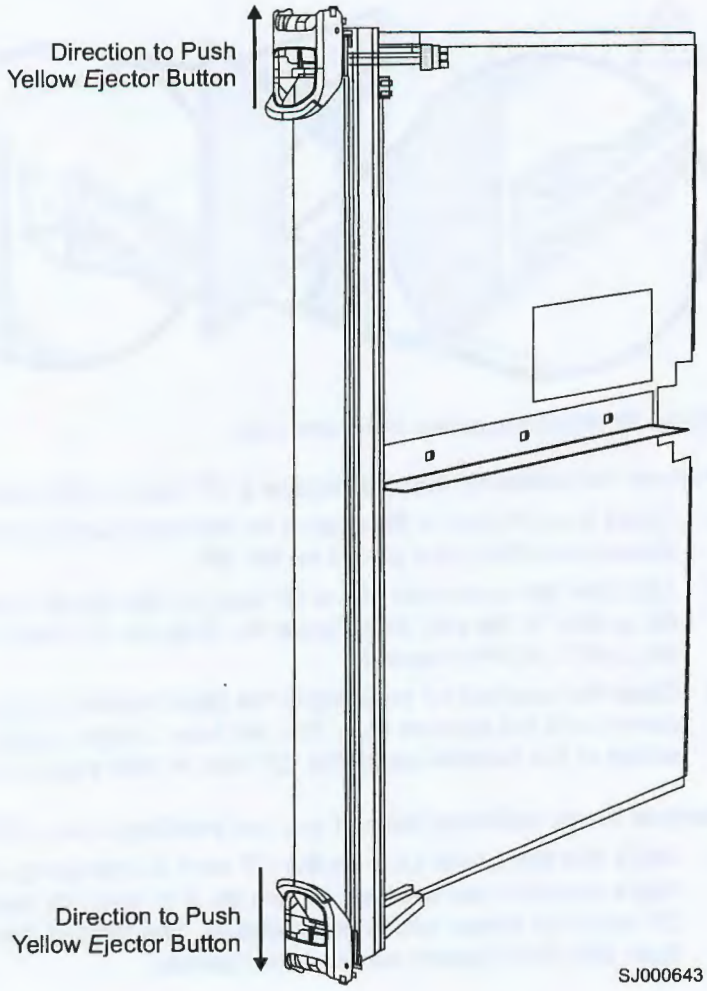


Figure 49. CP card filler panel with two ejectors

Replacing a CP card or filler panel

Attention: Do not force the installation. If the CP card or filler panel does not slide in easily, ensure that it is correctly oriented and aligned in the rail guides before you continue.

Figure 50 on page 82 shows the alignment guides in the card slots.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1322
Doc: 3690

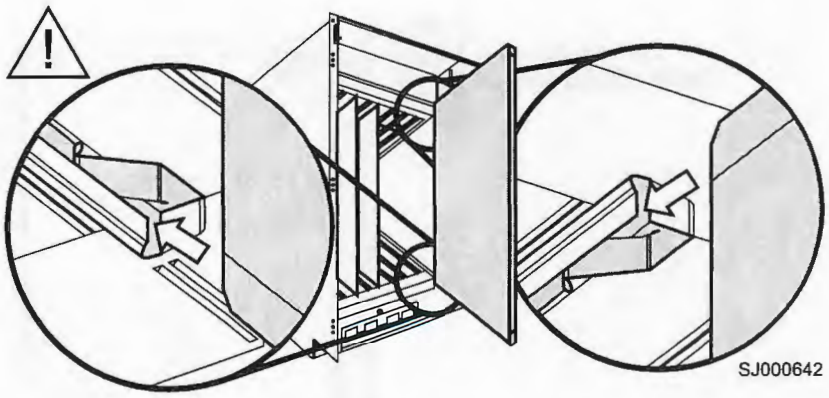


Figure 50. Alignment guides in the card slots

Perform the following steps to replace a CP card or filler panel:

1. Orient the CP card or filler panel so that the ejectors are at the front of the chassis and the metal pan is on the left.
2. Align the flat-metal side of the CP card or filler panel inside the upper and lower rail guides in the slot. See Figure 50. Slide the CP card or filler panel into the slot until it is firmly seated.
3. Close the ejectors by pressing in the black handles toward the CP card or filler panel, until the ejectors lock. You will hear a slight audible click. The levering action of the handles seats the CP card or filler panel in the chassis.

Perform these additional steps if you are installing a new CP card:

1. Verify that the power LED on the CP card is displaying a steady green light. It might require a few seconds to turn on. If it does not turn on, ensure that the CP card has power and is firmly seated. The front of the CP card should be flush with the adjacent cards or filler panels.

   Note: The LED patterns can temporarily change during a POST and other diagnostic tests.
2. Connect the cables as required to the CP card:

   Attention: Do not route the cables in front of the exhaust vent (located at the top of the port side of the chassis).
   - Modem cable to the modem serial port
   - Serial cable to the terminal serial port
   - Ethernet cable to the Ethernet port

Verifying the operation of the new CP card

Perform the following steps to verify that the new CP card is operational:

1. Verify that startup and POST are complete on the new CP card (a minimum of 3 minutes), and that the CP cards have achieved failover redundancy.
   a. Wait until the Status LEDs on both CP cards are not lit.

      If Fabric OS v4.0.2 or later firmware is installed on both CP cards, the Status LED for the active CP card displays orange until the active CP card is fully operational. The Status LED for the standby CP card displays orange until the CP cards have achieved failover redundancy.
   b. From the serial console for the active CP card (the CP card that was not replaced), run the **hashow** command and verify that the command output includes `HA Enabled Heartbeat Up`.

The message HA-state in sync also displays. If not, POST is not complete or the CP cards have not yet achieved redundancy. Wait a minute and re-run the command until you can verify that redundancy has been achieved. See the sample output from the **hashow** command before redundancy is achieved.

```
SW1:admin> haShow
Local CP (Slot 5, CP0): Active
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State not in sync
SW1:admin>
```

2. Run the **slotshow** command. The command output should show the new CP card as enabled, as the following output shows.

```
SW1:admin> slotShow
Slot Blade Type ID Status
--------------------------------
1 SW BLADE 2 ENABLED
2 SW BLADE 2 ENABLED
3 SW BLADE 2 ENABLED
4 SW BLADE 2 ENABLED
5 CP BLADE 1 ENABLED
6 CP BLADE 1 ENABLED
7 SW BLADE 2 ENABLED
8 SW BLADE 2 ENABLED
9 SW BLADE 2 ENABLED
10 SW BLADE 2 ENABLED
SW1:admin>
```

3. Determine the firmware version. For Fabric OS v4.0 and earlier, run the **version** command. For Fabric OS v4.0c and later firmware, run the **firmwareshow** command. Sample output for the **version** command and the **firmwareshow** command follows.

```
SW1:admin> version
Kernel: 2.4.2
Fabric OS: v4.0.0
Made on: Fri Feb 1 23:02:08 2002
Flash: Fri Feb 1 18:03:35 2002
BootProm: 3.1.13b
SW1:admin>

SW1:admin> firmwareshow
Local CP (Slot 5, CP0): Active
Primary partition: v4.0.2
Secondary Partition: v4.0.2
Remote CP (Slot 6, CP1): Standby
Primary partition: v4.0.2
Secondary Partition: v4.0.2
SW1:admin>
```

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1323
Doc: 3690

4. If the firmware versions on the replacement card do not match the active CP card, bring the replacement card to the same firmware level as the active card.
   a. Download the firmware by using either of the following command options:
      - Run the **firmwaredownload** command to download the firmware to both CP cards at the same time. Enter all requested information and choose the reboot option. If the switch is running Fabric OS v4.0.2 and later

firmware, a message displays that warns you that this command causes the active CP card to reset. If this message displays, type `Y` to continue.

- If the firmware version of the replacement card is v4.1 or earlier, run the **firmwaredownload -s** command to download the firmware to only one of the CP cards. Enter all requested information and choose the reboot option. See the following sample output for the **firmwaredownload** command.

```
SW1:admin> firmwaredownload
Server Name or IP Address: 123.456.78.90
User Name: user
File Name: /v4.0.2/release.plist
Password: xxxxxx
Full Install (Otherwise upgrade only) [Y]:
Do Auto-Commit after Reboot [Y]:
Reboot system after download [N]: y
Start to install packages......
dir ################################################
terminfo ############################################
...
glibc ###############################################
sin #################################################
Write kernel image into flash.
file verification SUCCEEDED
Firmwaredownload completes successfully.
SW1:admin>
```

5. Verify that the restart is complete and that the CP cards have achieved failover redundancy.
   a. Wait until the Status LEDs on both CP cards are not lit.
   b. Run the **hashow** command and verify that the command output includes `HA Enabled Heartbeat Up`. If not, wait a minute and then rerun the command until you can verify that redundancy is achieved.
6. Run the **version** or **firmwareshow** command to verify that the firmware version has been updated.
7. Create a serial connection to the new CP card, as shown in step 1 on page 82.
8. Log into the new CP card as `Admin` and type `0` to log into logical switch 0. See the following sample output.

```
Fabric OS (cp1)
cp1 Console Login: admin
Password:
Enter Switch Number to Login <0 or 1>: 0
SW0:admin>
```

9. From the serial console for the new CP card, run the **hafailover** command to fail the active CP card over to the new CP card.
10. Verify that the configuration has successfully propagated to the new CP card by checking any configuration parameters for which you have specified non-default values. To do this, run the **configshow** command, followed by a text string (in quotation marks) that relates to the parameter, for example, **configshow** "**fabric**". This limits the command output to entries that contain that text string.

Note: If you run the **configshow** command without a filter, it prints out approximately 1000 lines. For more information, see the *Brocade Fabric OS Reference*.

See the following sample output for the **configshow** command with the **"fabric"** as a filter.

```
SW0:admin> configshow "fabric"
fabric.domain:5
fabric.ops.BBCredit:16
fabric.ops.E_D_TOV:2000
fabric.ops.R_A_TOV:10000
fabric.ops.dataFieldSize:2112
fabric.ops.mode.fcpProbeDisable:0
fabric.ops.mode.isolate:0
fabric.ops.mode.longDistance:0
fabric.ops.mode.noClassF:0
fabric.ops.mode.tachyonCompat:0
fabric.ops.mode.unicastOnly:0
fabric.ops.mode.useCsCtl:0
fabric.ops.mode.vcEncode:0
...
SW0:admin>
```

11. Run the **haenable** command.
12. If the switch configuration does not replicate correctly, download the switch configurations that were backed up in step 8 on page 79.
    a. Run the **switchdisable** command to disable the current logical switch, which should still be switch 1.
    b. Run the **configdownload** command and enter the requested information.

       Note: If the switch is running Fabric OS v4.0.2, a message displays that cautions you about downloading the correct configuration file. If this message displays, type `Y` to continue.

    c. After the configuration is downloaded, run the **switchenable** command.
    d. Log into switch 0 and repeat steps 12a through 12c. See the following sample output for downloading the configuration to both logical switches.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1324
Doc: 3690

```
SW0:admin> switchdisable
SW0:admin> configdownload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
Committing configuration...done.
download complete
SW0:admin>
SW0:admin> switchenable
10 9 8 7 6 5 4 3 2 1
fabric: Principal switch
fabric: Domain 1
SW0:admin> login
cpl login: admin
Password:
Enter Switch Number to Login <0 or 1>: 1
SW1:admin>
SW1:admin> switchdisable
SW1:admin> configdownload
Server Name or IP Address [host]: 123.456.78.90
User Name [None]: user
File Name [config.txt]: config.txt
Password: xxxxxx
Committing configuration...done.
download complete
SW1:admin> switchenable
10 9 8 7 6 5 4 3 2 1
fabric: Principal switch
fabric: Domain 1
SW1:admin>
```

13. Pack the old CP card in the packaging that is provided with the new card. Return the old CP card by using your local return policy.

Replacing the CP card battery

Each CP card has a lithium carbon-monoflouride coin cell battery that has a 10-year life expectancy. If the real-time clock (RTC) loses time, you might need to replace the battery. Contact IBM if the RTC begins to lose time.

CAUTION:
Replace only with the same or equivalent type of battery that the manufacturer recommends. Discard used batteries according to the manufacturer's instructions.

Removing and replacing a power supply or filler panel

Use this procedure to remove and replace a power supply. The 2109 Model M12 can continue to operate during the replacement if at least one power supply continues operating for every four 16-port cards that are installed. You need a minimum of two power supplies.

Note: You do not need to notify the 2109 Model M12 of a hot-swap request before you remove a power supply. Power supply filler panels are not required to ensure correct air flow.

The left power connector provides power to the power supplies in slots 1 and 3. The right power connector provides power to the power supplies in slots 2 and 4. The power connectors and the power supply slots are color-coded to identify which power connectors provide power to which power supply slots. See Figure 15 on page 3 for the location of the power supplies.

Attention: To protect against ac failure, you need a minimum of one power supply in slot 1 or slot 3, and one power supply in slot 2 or slot 4. If only two power supplies are installed and they are both installed in slots corresponding to the same power cable, unplugging a single power cable will power down the entire chassis.

Attention: If adequate power is abruptly lost, such as through removal of a power supply, the entire switch is powered down. The power off order that the **powerOffListSet** command designates is not followed.

Attention: Disassembling any part of the power supply voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the power supply.

Time required

Less than 5 minutes

Removing a power supply or filler panel

Perform the following steps to remove a power supply or filler panel:

1. If the 2109 Model M12 is going to operate during the replacement procedure, check the LEDs to verify that the minimum of two power supplies are functioning before you uninstall the power supply.
2. Remove the power supply or filler panel from the chassis. See Figure 51 on page 88 for the location of the power supply.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº
1325
Doc: 3690

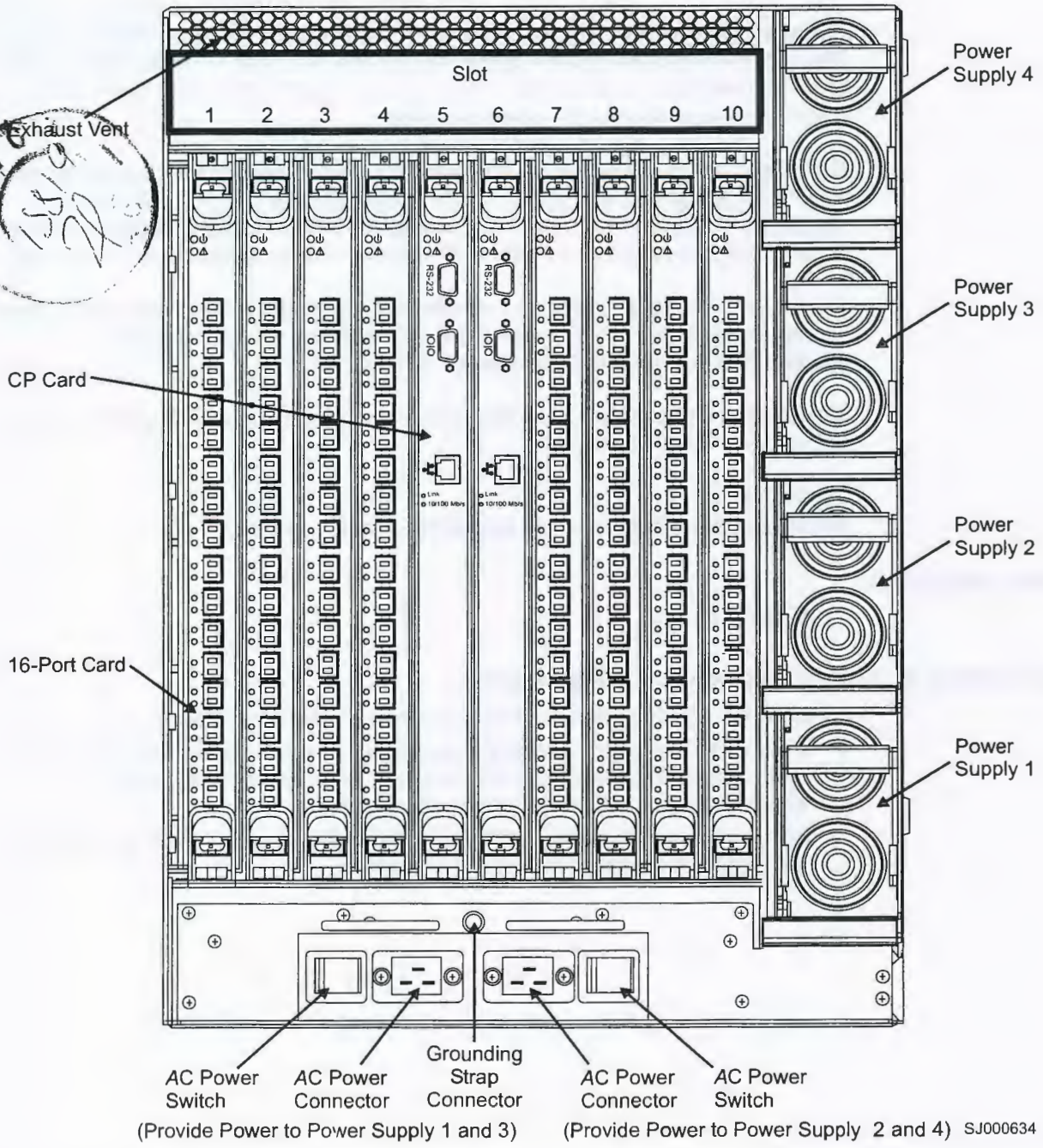


Figure 51. Location of the power supplies

Attention: Support the power supply from underneath while removing it from the chassis.

a. Remove the power supply by pushing the locking tab in towards the power supply then pull the handle out and down, and use the handle to pull the power supply out of the chassis. See Figure 52 on page 89.

b. Remove the filler panel by pulling it out by the handle.

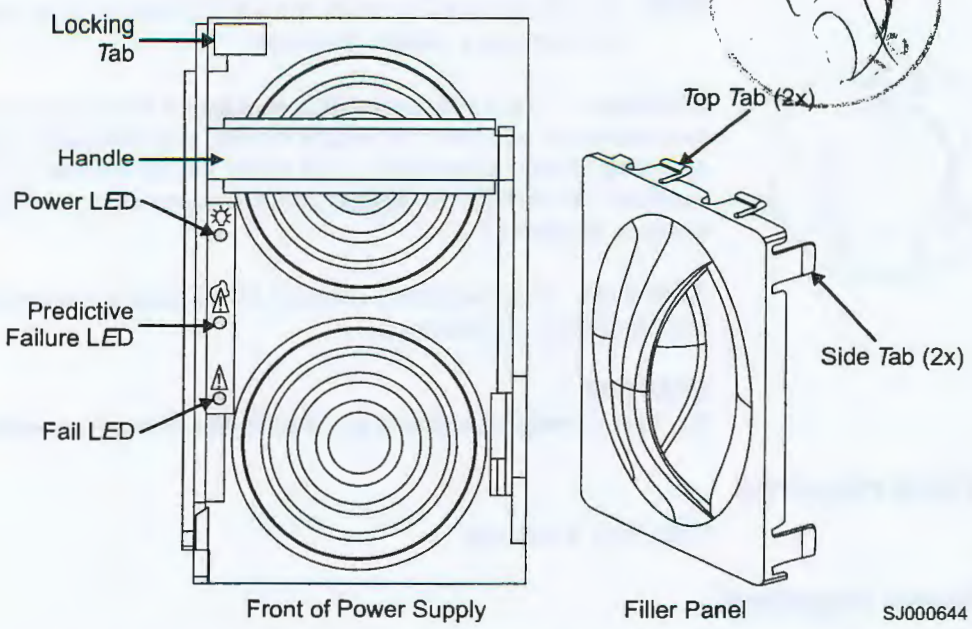


Figure 52. Power supply and filler panel

Replacing a power supply or filler panel

Attention: Do not force the installation of the power supply or filler panel. If the part does not install easily, ensure that it is properly oriented.

Perform the following steps to replace a power supply:

1. Orient the power supply so that the handle is toward the front of the chassis and the LEDs are on the left.
2. Unlock the handle and insert the power supply all the way into the slot.
3. Push the handle up until it clicks.
4. Verify that the power supply is seated by pulling gently on the handle.

Perform the following steps to replace a filler panel:

1. Orient the filler panel so that the handle is vertical and side tabs are on the right.
2. Push the filler panel into the slot.

Perform these additional steps if you are installing a new power supply:

1. Verify that the top LED on the power supply displays a steady green light.
2. If a green light is not displayed, ensure that both power cables are plugged in and that both ac switches are flipped to "|" (the ac switch lights up green).

Removing and replacing a blower assembly

Use this procedure to remove and replace the blower assembly. The 2109 Model M12 requires that a minimum of two of the three blower assemblies are operating. It can continue to operate during the replacement only if the other two blower assemblies continue to operate. If more than one blower must be turned off at the same time, you should turn off the 2109 Model M12 to prevent overheating.

BOS nº 03/2005 - CN - CPMI - CORREIOS
1326
Fls. Nº
Doc: 3690

Note: You do not need to notify the 2109 Model M12 of a hot-swap request before you remove a blower assembly.

Attention: The 2109 Model M12 requires a minimum of two operating blower assemblies at all times. To ensure continuous adequate cooling, maintain three operating blower assemblies at all times except for the brief period when replacing a blower assembly. The 16-port cards automatically shut down if the temperature range is exceeded.

Attention: Disassembling any part of the blower assembly voids the part warranty and regulatory certifications.

CAUTION:
No user-serviceable parts are inside the blower assembly.

Time required

Less than 5 minutes

Items required

#2 straight screwdriver

Removing a blower assembly

Perform the following steps to remove a blower assembly:

1. Before you remove the blower assembly, verify that the other two blower assemblies are functioning correctly. The blower assembly power LED should be steady green, and the fault LEDs should not be lit (see Figure 53 on page 91 for LED locations). For information about how to check the status of the blower assembly by using Telnet, see the *Brocade Fabric OS Reference*.
2. Remove the blower assembly from the chassis.

   CAUTION:
   Support the blower assembly from underneath while removing it from the chassis.

   a. Use the screwdriver to loosen the thumbscrews at the top and bottom of the blower assembly. See Figure 53 on page 91.
   b. Push in the top part of the handle. Pull out the lower part of the handle and pull the blower assembly out of the chassis.

Replacing a blower assembly

Attention: Do not force the installation. If the blower assembly does not slide in easily, ensure that it is properly oriented before you continue with the installation.

Perform the following steps to replace a blower assembly:

1. Orient the blower assembly. See Figure 53 on page 91.
2. Slide the blower assembly into the chassis, pushing firmly to ensure that it is seated.
3. Verify that the power LED displays a green light. If a green light is not displayed, ensure that the blower assembly is seated correctly.
4. Push the top of the handle into the recess.
5. Tighten the thumbscrews on the blower assembly to finger-tight.

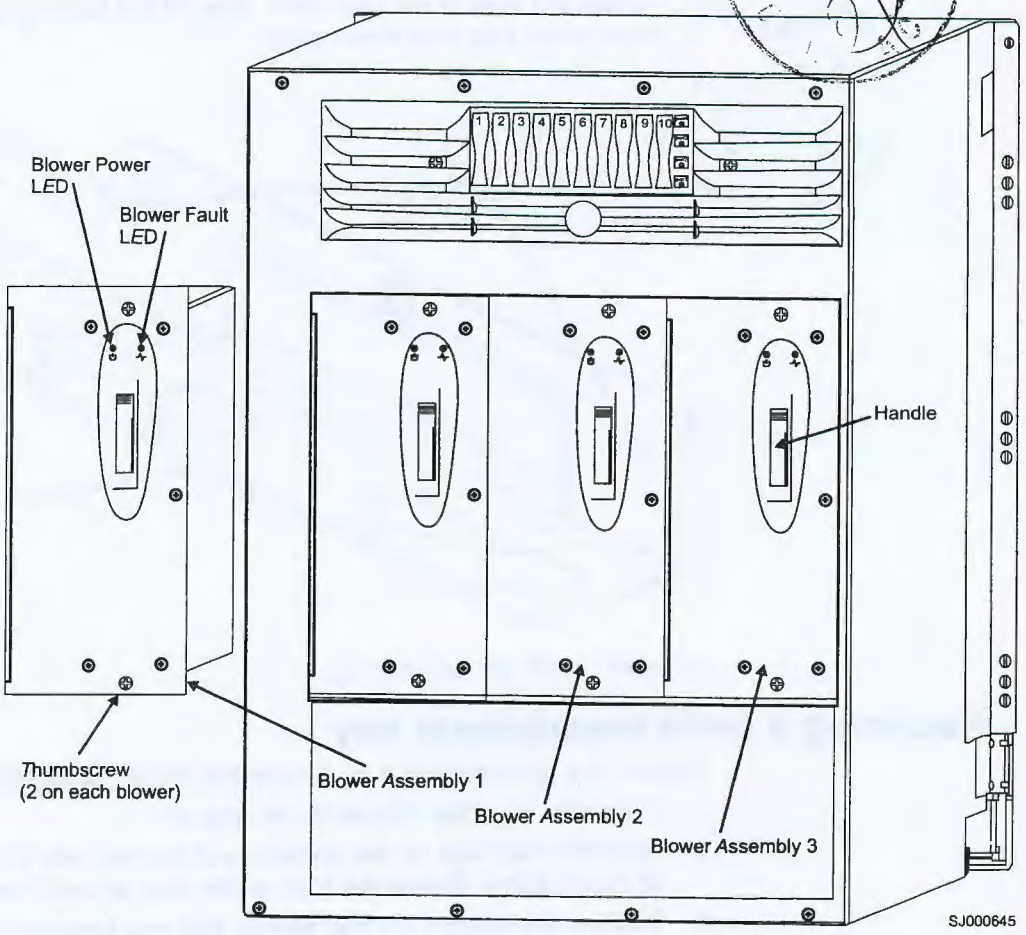


Figure 53. Blower assembly side of the 2109 Model M12 shown with one blower assembly uninstalled

Removing and replacing the cable management tray

Use this procedure to remove and replace the cable management tray. The 2109 Model M12 can continue to operate during the replacement.

Attention: Do not use a power screwdriver on the cable management tray.

Time required

Less than 5 minutes

Items required

#2 Phillips screwdriver

Removing a cable management tray

Perform the following steps to remove a cable management tray:

1. Pull any cables out of the cable management tray.
2. Unscrew the two screws that hold the tray to the chassis. See Figure 54 on page 92 for the location of the screws. Save the screws for reuse when you replace the cable management tray.

RQS nº 03/2005 - CN - CORREIOS
Fls. Nº 1327
Doc: 3690

3. Rotate the front of the tray down, then lift the back to disengage the tabs on the back of the tray from the chassis.

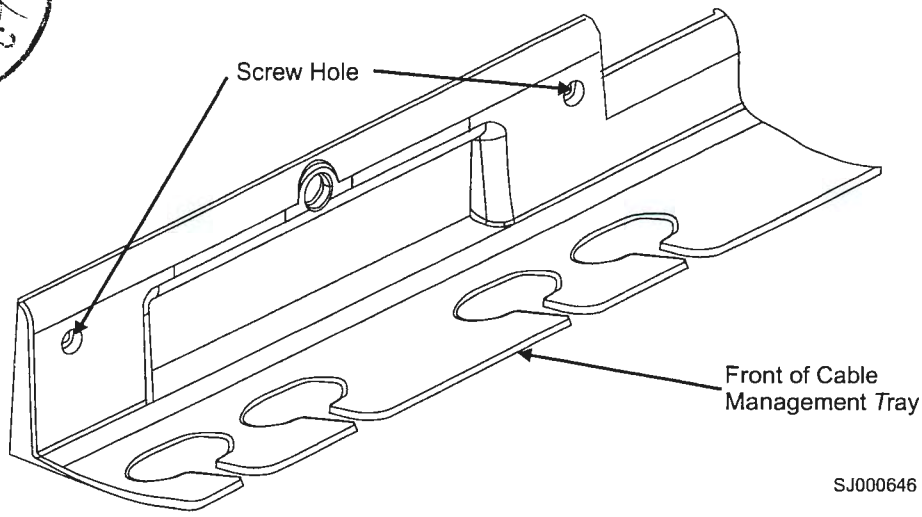


Figure 54. Cable management tray

Replacing a cable management tray

Perform the following steps to replace the cable management tray:

1. Orient the tray. See Figure 55 on page 93.
2. Insert the two tabs on the underside of the tray into the two slots at the bottom of the ac panel. Rotate the front of the tray up until it locks into place.
3. Position and tighten the two screws that you previously removed.
4. Arrange the cables through or along the tray as required.

Note: Route the power cables out each side of the chassis.

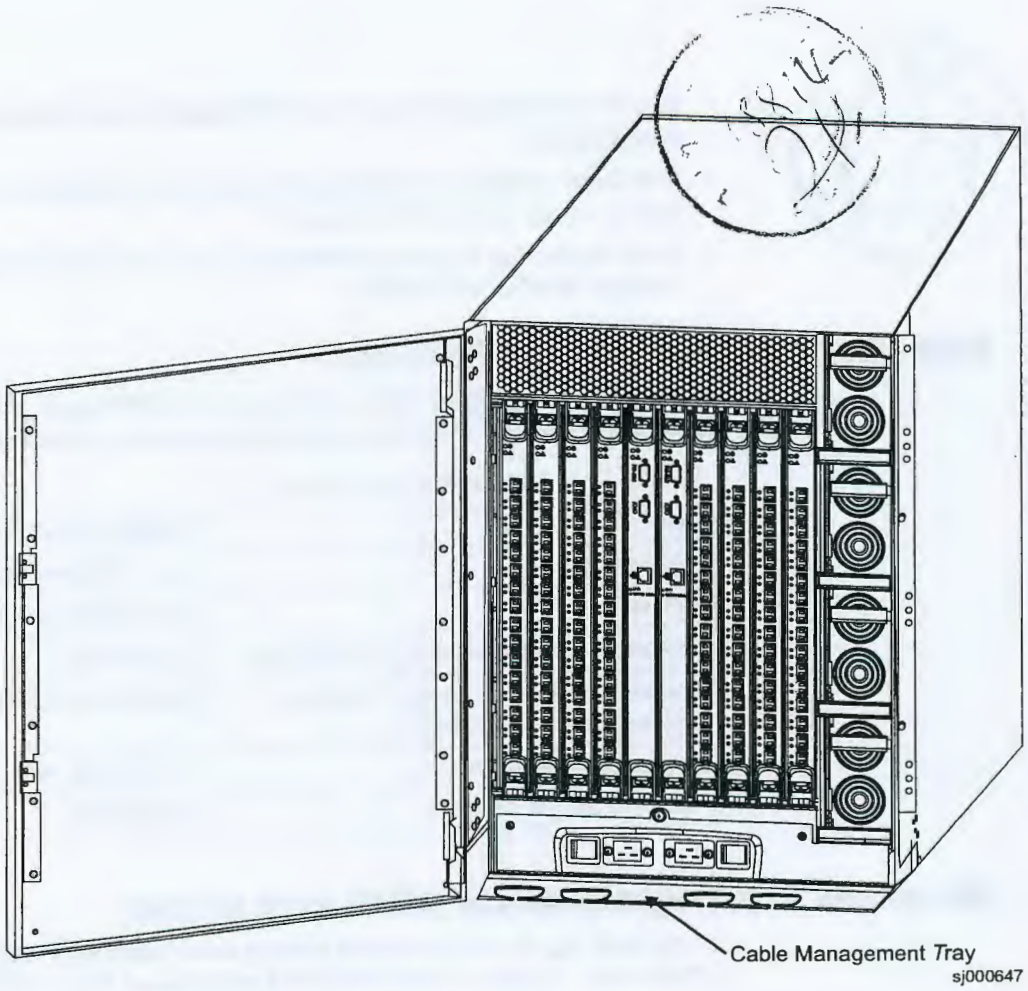


Figure 55. 2109 Model M12 with the cable management tray

Removing and replacing the WWN card

The WWN card is highly reliable. Before you replace the WWN card, verify that a replacement is necessary. If you are installing a new WWN card, the installation instructions are included with the product.

If you are going to replace a WWN card for Fabric OS earlier than v4.1.0, you must power down the 2109 Model M12. Do not remove the WWN card until you have received the replacement card. Do not restart the switch with a failed or missing WWN card.

Note: You must consult with Technical Support before you replace the WWN card.

Verifying if the WWN needs replacing

Ensure that the current card is firmly seated when you perform troubleshooting steps.

Note: You must consult with Technical Support before you replace the WWN card.

Any of the following events might indicate that the WWN card needs to be replaced:

- Visible mechanical damage to the WWN card

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1328
Doc: 3690

- Any of the Status LEDs on the WWN card do not reflect the actual status of the components
- Problems viewing or modifying the data that is stored on the WWN (see "Data that is stored on the WWN card")
- Error messages regarding WWN unit 1 or unit 2 (see Messages that might indicate WWN card failure)

Data that is stored on the WWN card

Table 9 shows the data that is stored on the WWN card. The WWN card might need to be replace if you have difficulty retrieving or modifying this data.

Table 9. Data that the WWN card stores

Data	Related Commands
WWN values	wwn, chassisshow
License keys	licenseshow, licenseadd, licenseremove
Data about the chassis and the WWN card	chassisshow
Ethernet and Fibre Channel IP address information for the CP cards	ipaddrshow, ipaddrset
History log information	historyshow, historylastshow
Names of logical switches	switchname

Messages that might indicate WWN card failure

If the error log or serial console display error messages that indicate problems with WWN unit 1 or unit 2, the WWN card might have failed. WWN unit 1 and unit 2 correspond to information that is specific to the WWN card, and are displayed by the **chassisshow** command. Table 10 shows messages that might indicate WWN card failure. For more information about error messages, see the *Brocade Diagnostics and System Error Message Reference*.

Note: WWN unit 1 and unit 2 do not correspond to the WWNs for logical switches 0 and 1.

Table 10. Sample error messages

Type of Message	Sample Error Message
WWN unit 1 or unit 2 fails its field replacable unit (FRU) header access	0x24c (fabos): Switch: 0, error EM-I2C_TIMEOUT, 2, WWN 1 I2C timed out: state 0x4
WWN unit 1 or unit 2 is being faulted	0x24c (fabos): Switch: 0, Critical EM-WWN_UNKNOWN, 1, Unknown WWN #2 is being faulted
WWN unit 1 or unit 2 is not present or is not accessible	0x24c (fabos): Switch: 0, Error EM-WWN_ABSENT, 2, WWN #1 not present
Writing to the FRU history log (hilSetFruHistory) has failed	0x24c (fabos): Switch: 0, Error EM-HIL_FAIL, 2, HIL Error: hilSetFruHistory failed, rc=-3 for SLOT 3

Removing and replacing the PDU

Use this procedure to remove and replace the PDU. See Figure 57 on page 116 and Figure 58 on page 117 for the orientation of the PDU and the power cords.

Removing the PDU

Complete the following steps to remove the PDU from the cabinet:

1. Follow the steps in "Power-off procedure" on page 70.
2. Turn off power and disconnect the ac power distribution bus from the customer's ac power outlet. Record the locations of the switch ac power cables that are plugged into the PDUs.
3. Unplug the switch ac power cables from the PDUs.
4. Remove the four mounting screws from the PDU. Pull the unit toward you.
5. Remove the PDU from the cabinet.
6. Remove the four M6 screws from the dual device attachment bracket (the center bracket attaching the two PDUs together). Set the screws aside for reuse when you replace the PDU.
7. Remove the two M3 x 5 screws from the dual-device attachment bracket of the PDU that you are replacing. Set the screws aside for reuse when you replace the PDU.
8. Remove the two M3 x 5 screws from the horizontal mounting bracket of the PDU that you are replacing (the bracket that is attached to the cabinet). Set the screws aside for reuse when you replace the PDU.

Replacing the PDU

Complete the following steps to replace a PDU in the cabinet:

1. Replace the horizontal mounting bracket on the new PDU by using the two M3 x 5 screws that you removed during the removal procedure.
2. Replace the dual device attachment bracket by using the two M3 x 5 screws that you removed earlier in the procedure.

   Note: Make sure that the threaded holes are on the opposite side of the device as the holes on the other attachment bracket.
3. Push the two PDUs together, aligning the holes on the dual device attachment brackets.
4. Secure the front and rear of the brackets to each other by using the four M6 screws that you removed during the removal procedure.
5. Slide the PDU into position. Install the four mounting screws.
6. Reconnect any power cables that you disconnected from the PDU.
7. Plug the power cables into the locations that you recorded during the removal procedure.
8. Follow the steps in "Power-on procedure" on page 69.

Removing and replacing the chassis door

Use this procedure to remove and replace the chassis door on the 2109 Model M12.

Note: The chassis door is required to ensure that the 2109 Model M12 meets electromagnetic interference (EMI) and other regulatory certifications.

Time required

Less than 5 minutes

- CN -
CPMI - CORREIOS
Fls. Nº 1329
Doc: 3690

Removing the chassis door

Perform the following steps to remove the chassis door:

1. Open the door 90°.
2. Support the door to prevent it from falling.
3. Push the spring-loaded lever on the upper hinge up and into the notch in the hinge.
4. Push the spring-loaded lever on the lower hinge down and into the notch in the hinge. Pull the door out, towards you.
5. Pull the door away from the chassis.

Replacing the chassis door

Perform the following steps to replace the chassis door:

1. Ensure that the levers on the spring-loaded pins on both hinges are pushed into the notches.
2. Align the spring-loaded pins with the chassis portion of the hinges.
3. Release the pins by pushing the levers out of the notches.

Removing and replacing the front or rear cabinet door

Use this procedure to remove and replace the front or rear cabinet doors.

Removing the cabinet door

Perform the following steps to remove the front or rear door:

1. Open the door of the cabinet.
2. Remove the door by lifting it up and out.
3. Remove the hinge bracket (if necessary) by removing the hinge mounting screws that attach the bracket to the rack. See Figure 56.

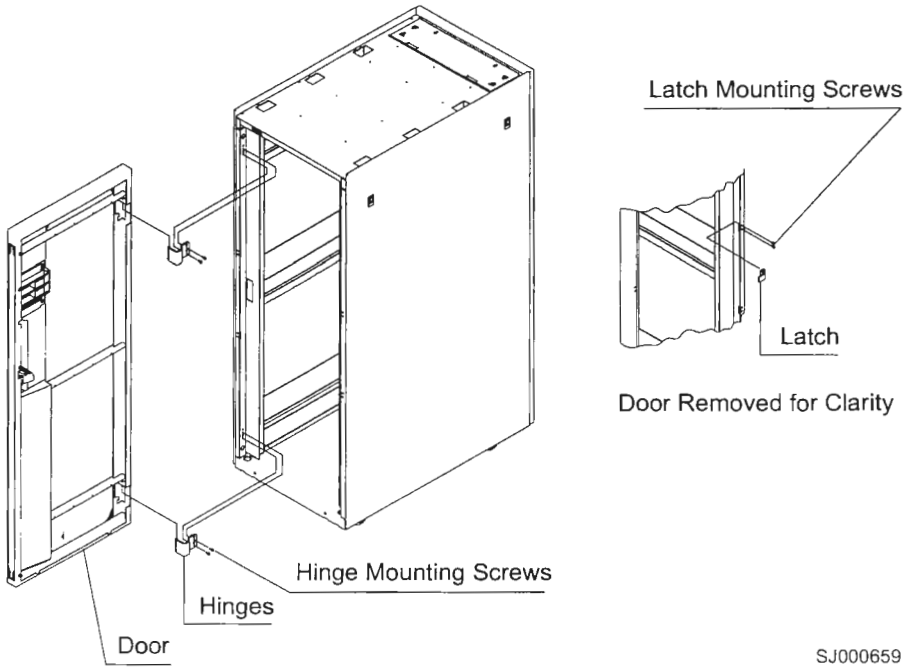


Figure 56. Removing the cabinet door

Replacing the cabinet door

Perform the following steps to replace the front or rear door:

1. Align the door with the hinge pin.
2. Install the bottom hinge pin (the longest pin) first.
3. Install the top hinge pin (the shortest pin) second.

Relocating the cabinet

Perform the following steps to relocate the cabinet:

1. Turn off all power to the cabinet and the 2109 Model 12 that is installed.
2. Disconnect all power and all device cables.
3. Unbolt the cabinet from the floor or remove the stabilizers.
4. Raise all the leveling feet.
5. Unlock each caster wheel by loosening the screw on the caster.
6. Move the cabinet to the new position.
7. Reposition the cabinet. Go to "Step 1. Position the cabinet" on page 7.

Reference information for the fruinfoset command

You must run the **fruinfoset** command through the active CP card by using root access. For more information, see Table 11.

Table 11. Reference information for the fruinfoset command

Name	fruinfoset
Syntax	`fruinfoset`
Availability	Factory or root only
Description	This command provides for the setting of the four externally modifiable fields in the header that is associated with each FRU. After the new data is written, the final contents of the fields are printed. No other fields can be modified. Some FRUs might not contain customer data or might not be programmable, in which case an error message displays.
Operands	**FRU ID** and **number** are the required operands. **FRU ID** Type of FRU: • Slot (port card or CP card in a slot) • Fan (blower assembly) • Ps (power supply) • Chassis (chassis or WWN card) **number** Physical slot or unit number for which the information will be input. For chassis information, type `chassis 1`. For WWN card information, type `chassis 2`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1330
3690
Doc:

Table 11. Reference information for the fruinfoset command (continued)

Usage	The modifiable fields and their maximum field sizes are as follows: **Field name** — **Maximum number of characters** ID — 10 characters PN (part number) — 20 characters SN (OEM serial number) — 20 characters RV (revision code — 4 characters Chassis SN (serial number) — 12 characters (This field displays only when the chassis 1 parameter is used.) These fields might not display for all FRUs. For each field that displays, the existing value displays followed by a > prompt for the new value. If more than the allowed number of characters are entered, the extra characters at the end are ignored, and a warning message displays. Leading blanks are also ignored. The `chassis SN` prompt displays only if the chassis 1 parameter is entered after the command. The usage rules are the same as for other values. The chassis serial number is identified by the **chassisShow** command as the `Serial Num for Chassis/WWN: Unit 1`

Appendix A. Product specifications

This appendix contains the 2109 Model C36 with Model M12 specifications.

2109 Model M12 components

The 2109 Model M12 contains the following components:

- A 14U chassis, designed to be mounted in a 48.26 cm (19 in.) rack. Two 2109 Model M12 switches can be mounted in a 2109 Model C36 cabinet.
- 16-port cards in configurations up to eight cards per chassis, with 16 optical ports per card, compatible with SFPs.
- Two CP cards, each with:
  - One modem serial port with a DB-9 connector (full RS-232)
  - One terminal serial port with a DB-9 connector (RS-232 signal subset)
  - One IEEE compliant RJ-45 connector for use with a 10 Mbps or 100 Mbps Ethernet connection
  - A real-time clock (RTC) with a 10-year battery and 56 bytes of NVRAM
- Four power supplies with built-in fans. The power supplies plug into internal blind-mate connectors when installed in the chassis.
- Two ac power inlet connectors with ac power switches (power panel).
- A WWN card and bezel.
- Three blower assemblies for forced-air cooling of the 16-port cards and the CP cards.

Air enters inlet vents on the blower assembly side of the chassis and exits through vents on the port side of the chassis. The blower speed is governed by inlet air temperature. The blowers go into high speed when the inlet air temperature exceeds 33°C (91°F).

Physical dimensions

The dimensions of the 2109 Model M12 are listed in Table 12.

Table 12. Physical dimensions of the 2109 Model M12

Dimension	Value
Height	14U (24.11 in.)
Depth	70.9 cm (27.9 in.)
Depth with door	72.9 cm (28.7 in.)
Width	43.7 cm (17.2 in.)

2109 Model M12 and component weights

The weight of a fully loaded 2109 Model M12, as well as the weights of individual components, are listed in Table 13.

Table 13. Component weights

Component	Weight
Fully loaded chassis	Approximately 114 kg (250.0 lbs)
Empty chassis	47.1 kg (104.0 lbs)

© Copyright IBM Corp. 2002, 2003

CPMI - CORREIOS
1331
Fls. Nº
Doc: 3690

Table 13. Component weights (continued)

Component	Weight
Door	3.4 kg (7.6 lbs)
Blower assembly	4 kg (8.8 lbs)
Power supply	3.2 kg (7.0 lbs)
WWN bezel	0.27 kg (0.6 lbs)
CP card	2.5 kg (5.6 lbs)
16-port card	3.9 kg (8.6 lbs)
Card filler panel	1.6 kg (3.2 lbs)
Cable management tray	0.27 kg (0.6 lbs)

2109 Model C36 with Model M12 specifications

The specifications for the 2109 Model C36 with Model M12 are listed in Table 14.

Table 14. 2109 Model C36 with Model M12 specifications

Dimension	Value
Height	1785 mm (70.3 in.)
Depth	• With rear door installed: 1042 mm (41 in.) • With rear and front door installed: 1098 mm (43.3 in.)
Width	• With side panels installed: 650 mm (25.6 in.) • Without side panel installed: 623 mm (24.5 in.)
EIA units	36 EIA units
Weight	Cabinet with two 2109 Model M12 switches: 816 kg (1795 lbs)

16-port card specifications

The ports in the 2109 Model C36 with Model M12 support full duplex link speeds at 2.125 Gbps or 1.0625 Gbps, inbound and outbound, automatically negotiating to the highest common speed of all the devices that are connected to the port. Each port has a serializer/deserializer (SERDES) which accepts 10-bit wide parallel data and serializes it into a high-speed serial stream. The parallel data is expected to be 8B/10B encoded data or equivalent.

The ports are compatible with optical SWL (780 - 850 nm), and optical LWL (1270 - 1350 nm), SFPs, and SFP-compatible cables. The strength of the signal is determined by the type of SFP that is being used.

The ports are universal and self-configuring, and are capable of becoming F_ports, FL_ports, or E_ports.

The ports meet all required safety standards. For more information about these standards, see Table 22 on page 106.

CP card specifications

This section describes the specifications for the CP card.

Memory specifications

The centralized memory maximizes switch throughput by guaranteeing full transmit and receive bandwidth to all Fibre Channel ports at all times.

Each CP card contains the type and specification of memory listed in Table 15.

Table 15. Memory specifications

Memory type	Amount
Main memory	256 MB of SDRAM (32 bits wide)
Flash memory	• User flash: 16 MB of 16-bit wide memory, stored in two 8 MB banks • Compact flash: 256 MB, partitioned in two 128 MB sections
Boot flash memory	512 KB of 8-bit wide memory for system startup

Battery specifications

The CP card has a lithium carbon-monoflouride coin cell battery.

Table 16 lists the battery specifications.

Table 16. Battery specifications

Type	Specification
Rayovac BR1225	3.0 volt, 50 mAh

CAUTION:
There is danger of explosion if the battery is incorrectly replaced. All used batteries must be discarded according to the manufacturer's instructions. Contact IBM if the real time clock begins to lose time.

Terminal serial port specifications

Each CP card provides a terminal serial port with a DB-9 connector with an RS-232 signal subset.

Note: For dust and ESD protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

The terminal serial port is intended primarily for use during the initial setting of the IP address and for service purposes.

A 3.0m (10 ft) serial cable is provided with the switch. You can convert it from a DB-9 serial cable to an RJ-45 style serial cable by removing the adapter on the end of the cable.

You can use the terminal serial port to connect to a computer workstation or terminal without connecting to the fabric. The terminal device should be configured to 9600 baud, 8 data bits, no parity, 1 stop bit, with no flow control.

The terminal serial port requires a straight through serial cable with a female 9-pin D-SUB connector. Use the pinouts listed in Table 17 on page 102.

CPMI - CORREIOS
Fls. Nº 1992
3690
Doc:

Table 17. Pinouts with signal and description

Pin	Signal	Description
1		
2	TxData	Transmit data
3	RxData	Receive data
4		
5	GND	Logic ground
6		
7		
8		
9		

Modem serial port specifications

Each CP card has a modem serial port (labeled RS-232) with a fully RS-232 compliant DB-9 connector.

Note: For dust and ESD protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

You can use the modem serial port to attach a modem to each CP card. The 2109 Model M12 detects modems only during the power-on or restart sequences, and automatically initializes them for operation. If modems are connected to an operating switch, a power on and off cycle, restart, or fast restart is required in order to detect the modems.

Customers should connect a "Y" cable on the telephone line to each modem. The active CP card answers on the first ring. The standby CP card answers on the seventh ring if the active CP card has failed to answer.

The modem serial port pinouts are listed in Table 18.

Table 18. Modem serial port pinouts

Pin	Signal	Description
1	DCD	Data carrier detect
2	RxData	Receive data
3	TxData	Transmit data
4	DTR	Data term ready
5	GND	Logic ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

Fibre Channel port specifications

The Fibre Channel ports in the Model M12 support full duplex link speeds at 2.125 Gbps or 1.0625 Gbps inbound and outbound. The ports automatically negotiate to the highest common speed of all devices that are connected to the port. Each port

has a SERDES that accepts 10-bit wide parallel data and serializes it into a high-speed serial stream. The parallel data is expected to be 8B/10B encoded data or equivalent.

The ports are compatible with the following SFPs and SFP-compatible cables:

- Optical SWL: 780 - 850 nm
- Optical LWL: 1270 - 1350 nm

The strength of the signal is determined by the type of SFP in use.

The ports are universal and self-configuring, and are capable of becoming F_ports, FL_ports, or E_ports. These ports meet all the required safety standards.

Facility specifications

To ensure correct operation of the 2109 Model C36 with Model M12 , ensure that the facility meets the following specifications:

- Power requirements for a physical inlet:
  - Input power requirements: 200 - 240 V ac, 24A, 50 - 60 Hz
  - Recommended power connector
- An adequate supply circuit, line fusing, and wire size, according to the electrical rating on the switch nameplate.
- An air flow of at least 350 cubic feet per minute per switch, available in the immediate vicinity of the 2109 Model C36 with Model M12.
- The power specifications listed in "Power specifications".
- The environmental specifications listed in "Environmental requirements" on page 104.
- Interference less than the standard levels listed in Table 21 on page 105, under Immunity.

Power specifications

CAUTION:
To remove power to the 2109 Model M12, disconnect both power cables.

The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections and distributed name server (DNS). It is electro-magnetic compatibility (EMC) compliant.

The power supplies are universal and capable of functioning worldwide without using voltage jumpers or switches. They meet IEC 61000-4-5 surge voltage requirements and are autoranging in terms of accommodating input voltages and line frequencies. Each power supply has its own built-in fan for cooling. The fans push the air towards the port side of the chassis.

The power specifications listed in Table 19 on page 104 are calculated for fully-loaded systems with four power supplies. A fully-loaded system has eight 16-port cards, two CP cards, and three blower assemblies.

Table 19 on page 104 lists the power specifications for the 2109 Model C36 with Model M12.

RQS nº 03/2005 - CN -
CPMI CORREIOS
1333
Fls. Nº
3690
Doc:

Table 19. Power specifications

Specification	Value
Total power available from each power supply	1 KW
Input voltage	200 - 240 V ac
Input line frequency	50 - 60 Hz
Harmonic distortion	Active power factor correction per IEC1000-3-2
Heat output (BTU rating)	• 64 ports: 1080 Watts, 3690 BTU per hour • 128 ports : 1960 Watts, 6700 BTU per hour
Maximum inrush current per power cord	40 amps peak
Input line protection	Thermal circuit breaker
Power supply dimensions	6.96 cm (2.74 in.) wide, 12.34 cm (4.86 in.) high, 34.29 cm (13.50 in.) long

Environmental requirements

Table 20 lists the environmental operating ranges for the 2109 Model C36 with Model M12. The requirements for non-operating conditions are also provided for acceptable storage and transportation environments.

Table 20. Environmental requirements

Condition	Acceptable range during operation	Acceptable range during nonoperation
Temperature (See Note)	0° - 40°C (40° - 104°F)	0° - 40°C (40° - 104°F)
Humidity	20% - 80% RH noncondensing, at 40°C	0% - 90% RH noncondensing, at 40°C
Altitude	0 - 3 km (0 - 10 000 ft) above sea level	0 - 12 km (0 - 39 370 ft) above sea level
Shock	4G, 11 MS duration, half-sine wave	0G, 11 MS duration, sq wave
Vibration	5G, 0 - 3 kHz at 1.0 octave per minute	10G, 0 - 5 kHz at 1.0 octave per minute
Heat dissipation	• 64 ports: 3690 BTU per hour • 128 ports: 6700 BTU per hour	Not applicable
Note: Temperature measured at the air inlets on the blower assembly side of the chassis.		

General specifications

Table 21 lists the general specifications for the 2109 Model C36 with Model M12.

Table 21. General specifications

Specification	Description
Configurable port types	The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections.
EMI rating	An operating 2109 Model C36 with Model M12 conforms to the EMI radiation levels specified by the following regulations: • FCC Rules and Regulations, Part 15B, Class A level • CISPR22 Class A • EN55022 Class A • VCCI Class A ITE • AS/NZS 3548 Class A • CNS13438 Class A • ICES-003 Class A
System architecture	Nonblocking shared-memory switch
System processor	IBM Power PC 405GP, 200 MHz CPU
ANSI Fibre Channel protocol	FC-PH (Fibre Channel Physical and Signaling Interface standard)
Modes of operation	Fibre Channel Class 2, Class 3, and Class F
Fabric initialization	Complies with FC-SW 5.0
Internet protocol (IP) over Fibre Channel (FC-IP)	Complies with FC-IP 2.3 of the FCA profile
Aggregate switch input/output (I/O) bandwidth	Per port: 4 Gbps, running at 2 Gbps, full duplex Per 16-port card: 64 Gbps, all 16 ports at 2 Gbps, full duplex
Port-to-port latency	Less than 2 microseconds with no contention (destination port is free)
Data transmission range	• Up to 500 m (1625 ft) for short wavelength optical link • Up to 10 km (32 820 ft) for long wavelength optical link
Immunity	• IEC 61000-4-2 Severity Level 3 for Electrostatic Discharge • IEC 61000-4-3 Severity Level 3 for Radiated Fields • IEC 61000-4-4 Severity Level 3 for Fast Transients • IEC 61000-4-5 Severity Level 3 for Surge Voltage • IEC 61000-4-6 Conducted Emissions • IEC 61000-4-11 Voltage Variations

CPMI - CORREIOS
1334
Fls: Nº
Doc: 3690

Table 21. General specifications (continued)

Specification	Description
Acoustics	When measured in EIA 4 of a 36 EIA TotalStorage rack, with front cover, and rear cover with acoustic baffle, declared sound power is LwAd = 7.5 B, average bystander sound pressure is LpA = 59 dBA.
Routing capacity	A minimum aggregate routing capacity of four million frames per second is provided for Class 2, Class 3, and Class F frames in a 64-port switch.

Regulatory specifications

The 2109 Model M12 is certified for the regulatory specifications that are listed in Table 22.

Table 22. Regulatory specifications

Country or region	Safety specification	EMC specification
Canada	CSA 22.2 No. 60950 Third Ed.	ICES-003 Class A
United States	UL 60950 Third Ed., Info. Tech. Equip.	FCC Part 15, Subpart B, (CFR title 47) Class A
Japan	IEC 60950+A1+A2+A3+A4+A11	VCCI V-3/2000.04, Class A
International	IEC 60950+A1+A2+A3+A4+A11	CISPR22 Class A
Norway	Nemko IEC 60950+A1+A2+A3+A4+A11 (CB Report)	

Table 22. Regulatory specifications (continued)

Country or region	Safety specification	EMC specification
European Union (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom)	73/23/EEC based on compliance to EN 60950:92 +A1:93+A2:93+A3:95+ A4:96+A11:97 (CB report inclusive of county deviations); TUV-GS (Germany)	89/336/EEC EN 55022:1998 Class A EN 55024 (Immunity) EN 60825-1:1994/A11, -2 EN 61000-4-2 Severity Level 3 for Electro Static Discharge EN 61000-4-3 Severity Level 3 for Radiated Fields EN 61000-4-4 Severity Level 3 for Electrical Fast Transients EN 61000-4-5 Severity Level 3 for Surge Voltage EN 61000-4-6 Conducted Emissions EN 61000-4-8 Magnetic Fields EN 61000-4-11 Line Interruption
Taiwan		BSMI Certification CNS 13438
Australia and New Zealand		AS/NZS 3548:1995 Class A (radio interference)

The 2109 Model C36 is certified for the following regulatory specifications:

- IEC 60950/EN 60950 Third Ed.
- CSA 60950-00/ANSI-UL 60950 Third Ed.
- CE (7/23/EEC based on EN 60950 Third Ed.; 89/336/EEC)

POST and Boot specifications

The Model M12 performs a POST by default each time that you power on (cold boot) or restart or reset the chassis. You can restart the Model M12 with the **switchreboot** command, the **reboot** command, or the **fastboot** command. The **fastboot** command restarts the switches without running POST. If you restart the active CP card, it fails over to the standby CP card.

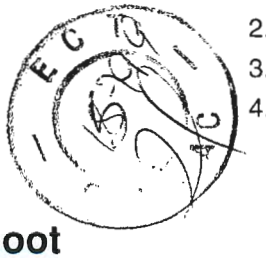
Monitoring POST results

You can monitor the success and failure of the diagnostic tests that are run during POST through LED activity, the error log, or a command line interface. POST requires a minimum of 3 minutes to complete, however the time might vary depending on the devices that are connected to the 2109 Model M12.

ROS P 03/2002 - CN - CPMI - CORREIOS
Fls. Nº 1335
Doc: 3690

POST performs the following steps:

1. Runs preliminary POST diagnostics
2. Initializes the operating system
3. Initializes the hardware
4. Runs diagnostic tests on several functions, including circuitry, port functionality, ability to send and receive frames, all aspects of memory, parity, statistics counters, and serialization



Boot

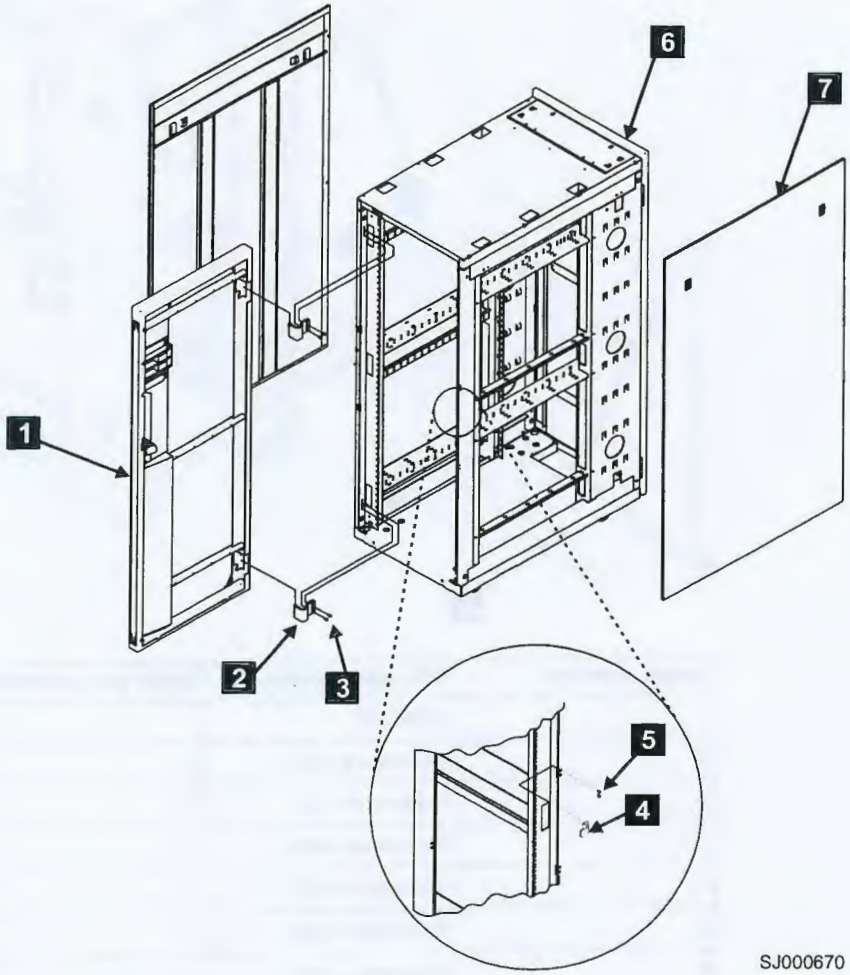
Boot completes in a minimum of 3 minutes if you run a POST. In addition to POST, boot includes the following steps after the POST completes:

1. Configures the universal port
2. Initializes the links
3. Analyzes the fabric. If any ports are connected to other switches, the switch participates in a fabric configuration.
4. Obtains a domain ID for the switch and assigns port addresses
5. Constructs unicast routing tables
6. Enables normal port operation

Appendix B. Parts information

This appendix contains detailed drawings, field replaceable unit (FRU) part numbers, and part descriptions for a 2109 Model C36 with Model M12.

Covers

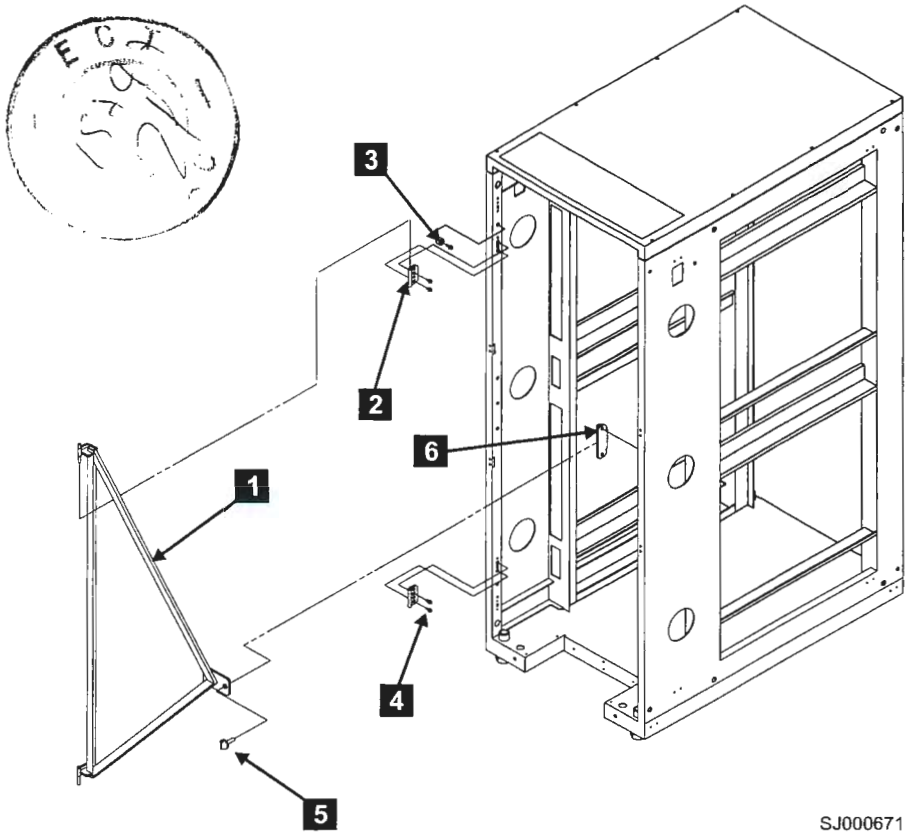


Index number	FRU part number	Units per assembly	Description
1	18P2120	1	Front door
2	31L7547	2	Hinge, front door
3	31L8594	4	Screw, front hinge
4	31L7545	1	Latch, front door
5	31L7540	2	Screw, front door latch
6	11P0724	1	Rear door (black)
7	05N6478	2	Side panel (black)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1336
3690
Doc:

© Copyright IBM Corp. 2002, 2003

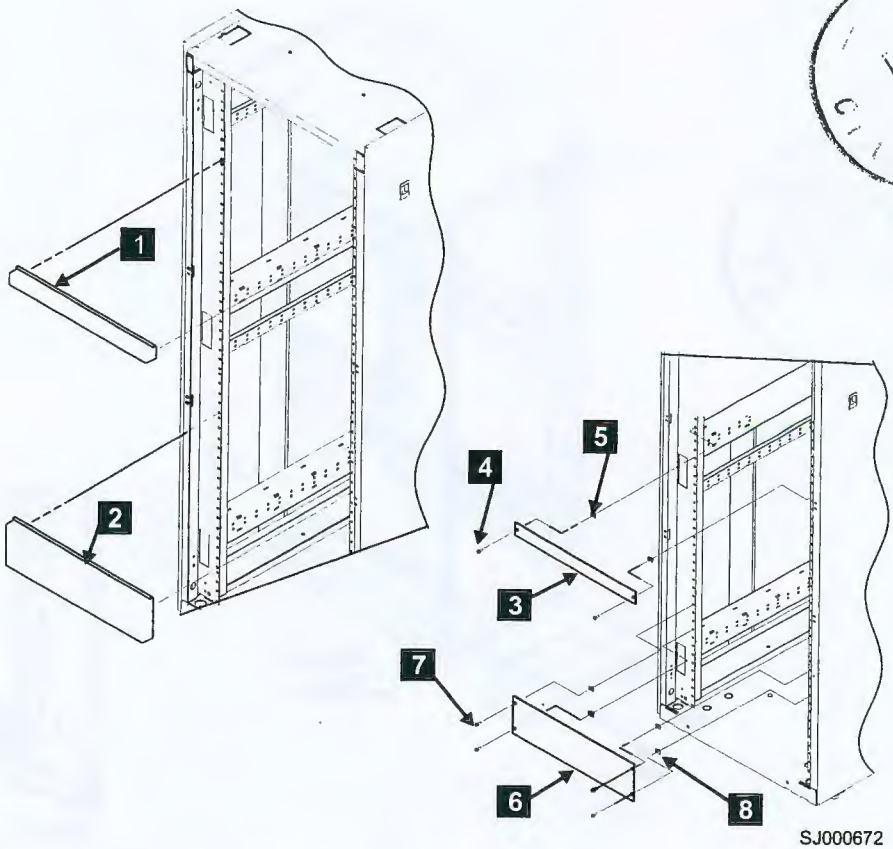
Earthquake brace



SJ000671

Index number	FRU part number	Units per assembly	Description
	05N4697	1	Earthquake brace kit
1	Reference only	1	Bracket
2	Reference only	2	Hinge
3	Reference only	1	Spacer
4	Reference only	7	Screw
5	Reference only	1	Bolt
6	Reference only	1	Latch plate

Blank fillers

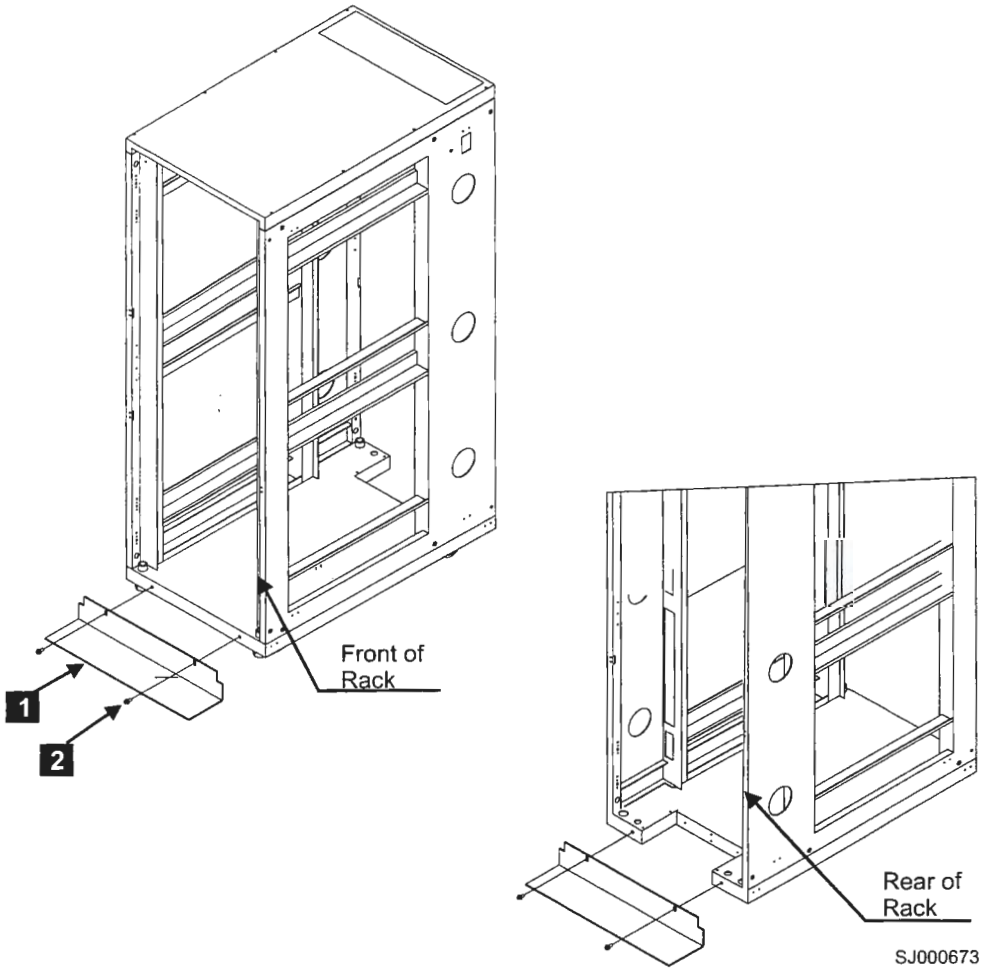


SJ000672

Index number	FRU part number	Units per assembly	Description
1	97H9754	As needed	1U (black) filler snap
2	97H9755	As needed	3U (black) filler snap
	18P2265	As needed	1U bolt in panel kit, (black)
3	Reference only	1	Panel (1U kit)
4	Reference only	2	M5 X 14 Hex screw (1U kit)
5	Reference only	2	M5 nut clip (1U kit)
	18P2233	As needed	3U bolt in panel kit, (black)
6	Reference only	1	Panel (3U kit)
7	Reference only	4	M5 X 14 hex screw (3U kit)
8	Reference only	4	M5 nut clip (3U kit)

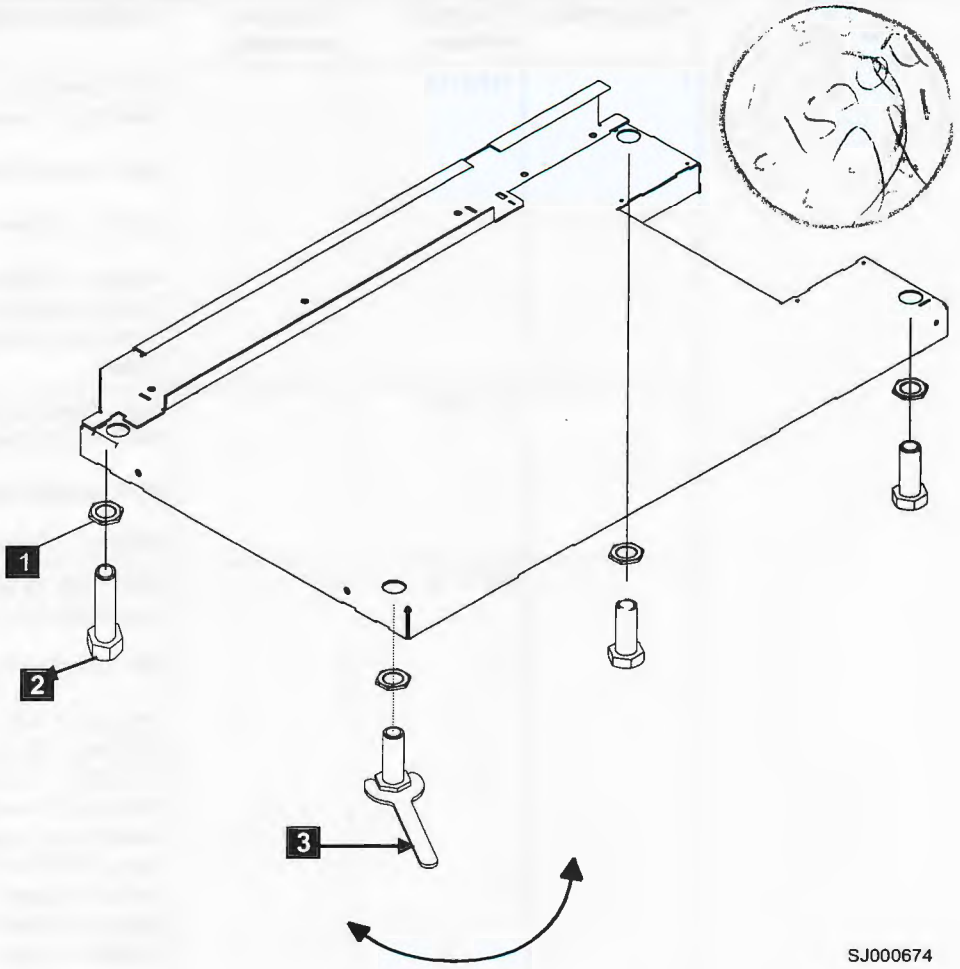
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1337
3690
Doc:

Stabilizers



Index number	FRU part number	Units per assembly	Description
	31L8305	1	Stabilizer kit (black)
1	Reference only	2	Bracket
2	Reference only	4	M8 X 25 screw, button head socket

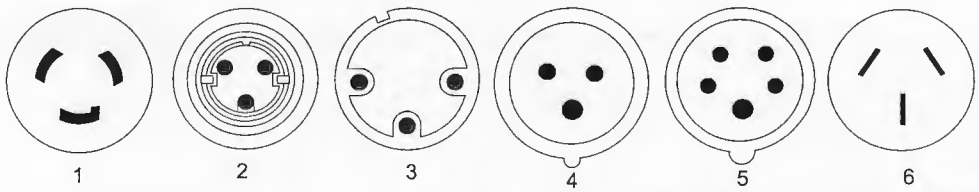
Leveling feet



SJ000674

Index number	FRU part number	Units per assembly	Description
1	Reference only	4	Jam nut
2	Reference only	4	Leveller
3	31L8313	1	Wrench

Power cords



SJ000675

RDS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1338
3690

Index number	FRU part number	Units per assembly	Country or region
1	11F0113	1	U.S. Standard, type 12 plug, L6-30P twist-lock connector, 14 ft cord 30 A, single phase U.S.A., Canada Anguilla, Antigua, Cape Verde Islands, Cayman Islands, French Polynesia, Honduras, Montserrat, St. Kitts and Nevis, Tortola
1	11F0114	1	U.S., Chicago, type 12 plug, L6-30P twist-lock connector, 6 ft cord 30 A, single phase Chicago, Illinois, U.S.A.
1	11F0115	1	AFE, type 12 plug, L6-30P twist-lock connector, 14 ft cord 30 A, single phase Argentina, Bahamas, Bangladesh, Barbados, Bermuda, Bolivia, Chile, China, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Honduras, Hong Kong S.A.R. of China, India, Indonesia, Jamaica, Japan, Macau S.A.R. of China, Malaysia, Mexico, Myanmar, Netherlands Antilles, Panama, Peru, Philippines, Singapore, Sri Lanka, Suriname, Taiwan, Thailand, Trinidad, Venezuela
N/A	18P2257	1	Universal without wall plug connector (non-US or Canada)
3	11F0106	1	30 A, single phase, PDL connector Wilco WP, type PDL plug, 14 ft cord Australia
3	11F0107	1	30 A, single phase, PDL connector Wilco WP, type PDL plug, right angle, 14 ft cord New Zealand

Index number	FRU part number	Units per assembly	Country or region
4	31F4466	1	32 A, single phase, three pin connector IEC 309, type 46 connector (2 power + ground), 14 ft cord Belgium, Bahrain, Botswana, Brazil, Egypt, Ethiopia, France, Ghana, Germany, Greece, Iceland, Iraq, Ireland, Italy, Jordan, Kenya, Kuwait, Lebanon, Malawi, Nigeria, Norway, Oman, Qatar, Saudi Arabia, Spain, Sudan, Tanzania, Uganda, United Kingdom, United Arab Emirates, Zaire, Zambia, Zimbabwe
N/A (See Note)	18P2257	1	Switzerland
6	87G6067	1	30 A, single phase Type KP connector, right angle, 14 ft cord Korea
Note: Install according to the national electrical code of the specific country or region.			

Cabinet parts list

Table 23 lists the items that are supplied with the 14U chassis mount kit.

Table 23. Items supplied with the 14U chassis mount kit

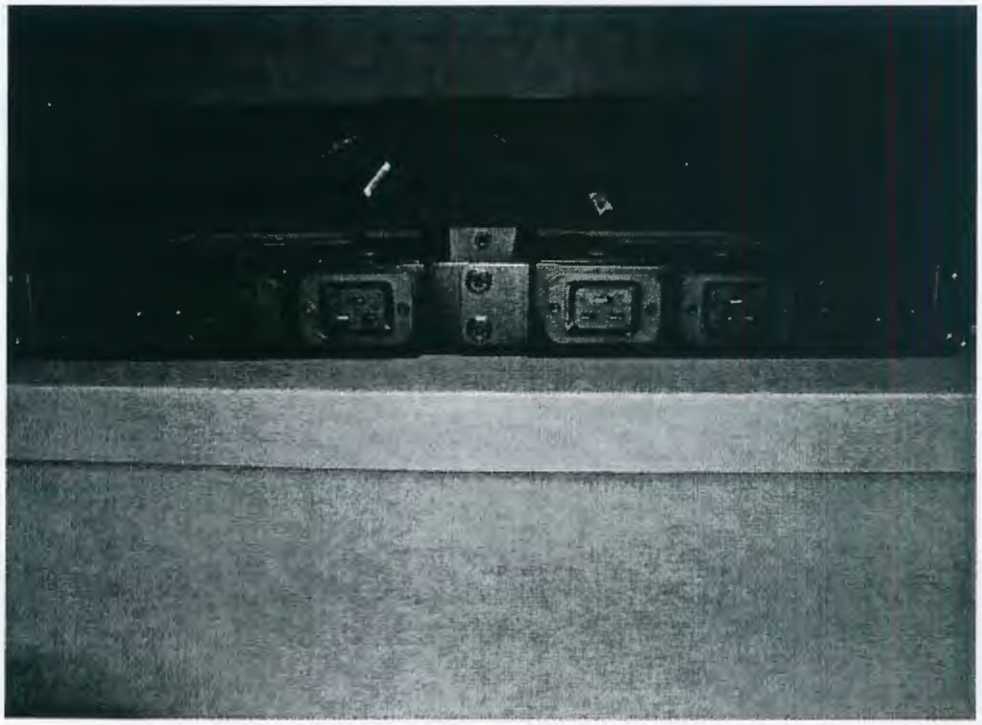
Item No.	Description	Quantity
1	Left mount shelf bracket	1
2	Right mount shelf bracket	1
3	Left upper mount bracket assembly, containing:	1
3a	Left upper mount bracket (flat)	1
3b	Left upper mount bracket (L-shaped)	1
3c	Screw	2
4	Right upper mount bracket assembly, containing:	1
4a	Right upper mount bracket (flat)	1
4b	Right upper mount bracket (L-shaped)	1
4c	Screw	2
5	10-32 x 5/16-in. Phillips flathead screw	8
6	10-32 x 5/8 in. Phillips panhead screw with washer	4
7	10-32 clip nut (package of 20; only four are required)	20

CPMI - CORREIOS
Fls N° 1359
3690
Doc:

Table 23. Items supplied with the 14U chassis mount kit (continued)

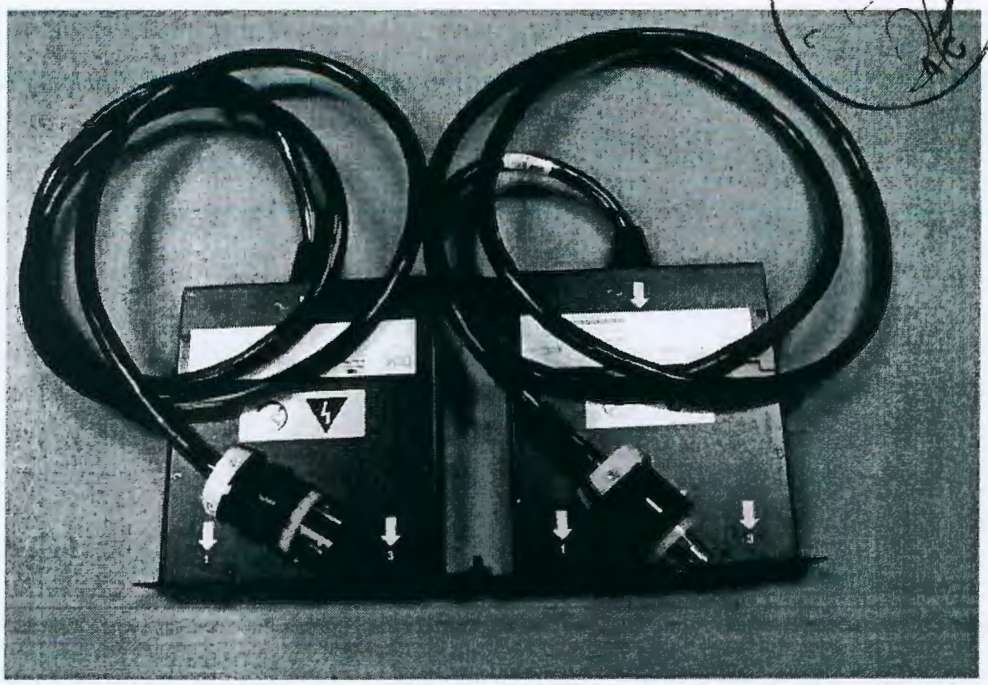
Item No.	Description	Quantity
8	1/4-20 x 1/2 in. Phillips panhead screws, with lock washer	16
Discard the following		
9	10-32 retainer nuts	4
10	1/4-20 x 1/2 in. Phillips panhead screws with glue	16
11	0.375 in. square washers	16
12	8-32 x 5/16 in. Phillips flathead screws	8

Power distribution unit (PDU)



SJ000652

Figure 57. Front view of the PDU



SJ000653

Figure 58. Top view of the PDU

FRU part number	Units per assembly	Description
32P1077	2 each	PDU, Winchester (PDU chassis)
24P6847	2 each	Power cord, PDU

2109 Model M12 parts list

FRU part number	Units per assembly	Description
18P5017	4 each	Switch blade, 16 port, 2 GB
18P5032	1 each	Chassis door
18P5034	4 each	Filler panel, switch blade, 16 port, 2 GB
18P5035	2 each	Blade, control processor
18P5037	3 each	Power supply, 180 - 264 V ac, 1000 watts
18P5039	3 each	Blower assembly
18P5126	1 each	Rear LED status panel card
18P5128	1 each	Chassis (including the backplane, blower and power supply backplane, ac and blower harness)
18P5130	1 each	Rear WWN bezel
18P5131	1 each	Tray, cable management

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1340
Fls. Nº
3690
Doc:

Appendix C. Blank planning worksheets

This appendix contains the following blank worksheets that you can use when you plan the installation of a 2109 Model C36 with Model M12:

- Planning worksheet
- Port configuration worksheet
- Zone definition worksheet
- Zone configuration worksheet

Make as many copies of the blank worksheets as you need to plan the installation of your switches. Give your system administrator copies of the completed worksheets.

Planning worksheet

Table 24. Planning worksheet

Item	Description
Firmware level	
Firmware location:	
Server name	
Username	
Directory	
Switch name	
Domain ID	
FCnetID (Fibre Channel IP address)	
FC netmask	
WWN	
Role	
Syslog daemon IP address	
Users defined - access level	
SNMP information:	
System description	
System contacts	
System location	
Event trap level 0 - 5	
Enable authentication traps	
RW community string	
RO community string	
Trap recipients IP address	
License keys	

RQS nº 03/2005 - CN - CPMI - CORREIOS
1341
Fls. Nº
3690
Doc:

© Copyright IBM Corp. 2002, 2003

Port configuration worksheet

Table 25. Port configuration worksheet

Port number	Device name	Device port	Cable length	Port type	Notes	Cable number
0						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Zone definition worksheet

Table 26. Zone definition worksheet

Zone member type (switch, port, WWN)	Zone member	Zone configuration name	Comments
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1342
3690
Doc:

Zone configuration worksheet

Table 27. Zone configuration worksheet

Zone member type (switch, port, WWN)	Zone member	Zone configuration name	Connects to
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			
Port (ID, P)			

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1343
3690
Doc:

© Copyright IBM Corp. 2002, 2003

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM
TotalStorage

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission statements

This section gives the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada compliance statement

Avis de conformite a la reglementation d'Industrie Canada: Cet appareil numerique de la classe A est conform a la norme NMB-003 du Canada.

Chinese Class A compliance statement

Attention: This is a Class A statement. In a domestic environment, this product might cause radio interference in which case the user might be required to take adequate measures.

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

European Community compliance statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product is in conformity with the EU council directive 73/23/EEC on the approximation of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits. This conformity is based on compliance with the following harmonized standard: EN60950.

This product has been tested and found to comply with the limits for class A Information Technology Equipment according to European Standard EN 55022. The limits for class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Where shielded or special cables (for example, cables fitted with ferrites) are used in the test to make the product comply with the limits:

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

Germany compliance statement

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische

Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG das

EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuellt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

ROS nº 03/2005 - CN - CPMI - CORREIOS
1344
Fls Nº
3690
Doc:

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:_|t¹|

"Geraete duerfen an Orten, fuer die sie nicht ausreichend entstoert sind, nur mit besonderer Genehmigung des Bundesministeriums fuer Post und Telekommunikation oder des Bundesamtes fuer Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Stoerungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs.4)

Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden

Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Nach der EN 55022:

"Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstoerungen verursachen. in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzufuehren und dafuer aufzukommen."

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen, sind die Geraete wie in den Handbuechern angegeben zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Government Ministry of Communication (MOC) statement

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this is not suitable for your use, you may exchange it for one with a non-business use.

Taiwan class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。 VS07171L

Glossary

This glossary provides definitions for the Fibre Channel and switch terminology used for the IBM 2109 Model M12. This glossary also provides definitions for the Fibre Channel and switch terminology used for the IBM TotalStorage SAN Cabinet 2109 Model C36.

This glossary defines technical terms and abbreviations used in this document. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at www.ibm.com/networking/nsg/nsgmain.htm

This glossary also includes terms and definitions from:

- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms*. New York: McGraw-Hill, 1994.

The following cross-reference conventions are used in this glossary:

See Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

See also Refers you to a related term.

8b/10b encoding. An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports

16-port card. The Fibre Channel port card provided with the 2109 Model M12. Contains 16 ports and the corresponding light-emitting diodes (LEDs). See also *port card.*

access control list (ACL). Enables an organization to bind a specific worldwide name (WWN) to a specific switch port or set of ports, preventing a port in another physical location from assuming the identity of a real WWN. Can also refer to a list of the read/write access of a particular community string. See also *device connection controls.*

account level switches. Switches that have four login accounts into the operating system (in descending order): root, factory, admin, and user. See also *admin account.*

ACL. See *access control list.*

address identifier. A 24-bit or 8-bit value used to identify the source or destination of a frame.

admin account. A login account intended for use by the customer to control switch operation. See also *account level switches.*

alias. An alternate name for an element or group of elements in the fabric. Aliases can be used to simplify the entry of port numbers and worldwide names (WWNs) when creating zones.

alias address identifier. An address identifier recognized by a port in addition to its standard identifier. An alias address identifier can be shared by multiple ports.

alias AL_PA. An arbitrated loop physical address (AL_PA) value recognized by a loop port (L_port) in addition to the AL_PA assigned to the port. See also *arbitrated loop physical address.*

alias server. A fabric software facility that supports multicast group management.

AL_PA. See *arbitrated loop physical address.*

American National Standards Institute (ANSI). The governing body for Fibre Channel standards in the U.S.A.

ANSI. See *American National Standards Institute.*

API. See *application programming interface.*

application programming interface (API). A defined protocol that allows applications to interface with a set of services.

application-specific integrated circuit (ASCI). In computer chip design, an integrated circuit created by first mounting an array of unconnected logic gates on a substrate and later connecting these gates in a particular configuration for a specific application. This design approach allows chips for a variety of applications to be made from the same generic gate array, thereby reducing production costs.

ARB. See *arbitrate primitive signal.*

© Copyright IBM Corp. 2002, 2003

CPMI
Fls. Nº
Doc: 3690 127

arbitrate primitive signal (ARB). A primitive signal that is transmitted as the fill word by a loop port (L_port) to indicate that the L_port is arbitrating to access to the loop. Applies only to the arbitrated loop topology.

arbitrated loop. A shared 100 MBps Fibre Channel transport structured as a loop and supporting up to 126 devices and one fabric attachment. A port must successfully arbitrate before a circuit can be established.

arbitrated loop physical address (AL_PA). An 8-bit value used to uniquely identify an individual port within a loop. A loop can have one or multiple AL_PAs.

arbitration wait timeout value (AW_TOV). The minimum time an arbitrating loop port (L_port) waits for a response before beginning loop initialization.

area number. A number that is assigned to each potential port location in the switch. Used to distinguish ports that have the same port number but are on different port cards.

ASIC. See *application-specific integrated circuit.*

asynchronous transfer mode (ATM). A broadband technology for transmitting data over local area networks (LANs) or wide area networks (WANs), based on relaying cells of fixed size. Provides any-to-any connectivity, and nodes can transmit simultaneously.

ATM. See *asynchronous transfer mode.*

auto-negotiate speed. Process that allows two devices at either end of a link segment to negotiate common features, speed (for example, 1 Gbps or 2 Gbps) and functions.

autoranging. A power supply that accommodates different input voltages and line frequencies.

autosense. Process during which a network device automatically senses the speed of another device.

AW_TOV. See *arbitration wait timeout value.*

backup FCS switch. The switch or switches assigned as backup in case the primary fabric configuration server (FCS) switch fails. See also *fabric configuration server switch* and *primary FCS switch.*

bandwidth. (1) The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). (2) The range of transmission frequencies available to a network. See also *throughput.*

basic input/output system (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BB_credit. See *buffer-to-buffer credit.*

beacon. When all the port light-emitting diodes (LEDs) on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by Telnet command or through Web Tools.

beginning running disparity. The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. See also *disparity.*

BER. See *bit error rate.*

BIOS. See *basic input/output system.*

BISR. Built-in self-repair.

bit error rate (BER). The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted. See also *error.*

blade. One component in a system that is designed to accept some number of components (blades). Blades could be individual servers that plug into a multiprocessing system or individual port cards that add connectivity to a switch. A blade is typically a hot swappable hardware device. See *16-port card.*

blind-mate connector. A two-way connector used in some switches to provide a connection between the system board and the power supply.

block. As applies to fibre channel, upper-level application data that is transferred in a single sequence.

bloom. Application-specific integrated circuit (ASIC) technology that the 2109 Model M12 is based on.

boot flash. Flash memory that stores the boot code and boot parameters. The processor runs its first instructions from boot flash. Data is cached in random access memory (RAM).

boot monitor. Code used to initialize the control processor (CP) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

British thermal unit (BTU). A measurement of heat produced in one hour.

broadcast. The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *multicast* and *unicast.*

BTU. See *British thermal unit.*

buffer-to-buffer credit. The number of frames that can be transmitted to a directly-connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. See also *buffer-to-buffer flow control.*

buffer-to-buffer flow control. Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. See also *buffer-to-buffer credit.*

CAM. Content addressable memory.

cascade. Two or more interconnected Fibre Channel switches that can build large fabrics. Switches can be cascaded up to 239 switches, with a recommended maximum of seven inter-switch links (no path longer than eight switches). See also *fabric* and *inter-switch link.*

central processing unit (CPU). A part of a computer that includes the circuits that control the interpretation and execution of instructions. A CPU in the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

chassis. The metal frame in which the switch and switch components are mounted.

circuit. An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions. See also *link.*

class 1. Service that provides a dedicated connection between two ports (also called connection-oriented service), with notification of delivery or nondelivery.

class 2. Connectionless service between ports with notification of delivery or nondelivery.

class 3. Connectionless service between ports without notification of delivery. Other than notification, the transmission and routing of class 3 frames is the same as class 2 frames.

class F. Connectionless service for inter-switch control traffic. Provides notification of delivery or nondelivery between two expansion ports (E_ports).

class of service. A specified set of delivery characteristics and attributes for frame delivery.

CLI. See *command line interface.*

CMI. Control message interface.

comma. A unique pattern (either 1100000 or 0011111) used in 8b/10b encoding to specify character alignment within a data stream. See also *K28.5.*

command line interface (CLI). Interface that depends entirely on the use of commands, such as through Telnet or simple network management protocol (SNMP), and does not involve a graphical user interface.

community (SNMP). A relationship between a simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

compact flash. Flash memory that stores the run-time operating system and is used like hard disk storage. Not visible within the memory space of the processor. Data is stored in file system format. Also called user flash.

control processor (CP). The central processing unit that provides all control and management functions in a switch.

control processor card (CP card). The central processing unit of the 2109 Model M12, which contains two control processor (CP) card slots to provide redundancy. Provides Ethernet, serial, and modem ports with the corresponding light-emitting diodes (LEDs).

core switch. A switch whose main task is to interconnect other switches. Also referred to as a backbone switch. See also *edge switch.*

CP. See *control processor.*

CP card. See *control processor card.*

CPLD. Complex programmable logic device.

CPU. See *central processing unit.*

CRC. See *cyclic redundancy check.*

credit. When applied to a switch, the maximum number of receive buffers provided by a fabric port (F_port) or fabric loop port (FL_port) to its attached node port (N_port) or node loop port (NL_port), respectively, such that the N_port or NL_port can transmit frames without over-running the F_port or FL_port.

CSA. Canadian Standards Association.

cut-through. A switching technique that allows the route for a frame to be selected as soon as the destination address is received. See also *route.*

cyclic redundancy check (CRC). A check for transmission errors included in every data frame.

data communications equipment (DCE) port. A port that is capable of interfacing between a data terminal equipment (DTE) port and a transmission circuit. DCE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *data terminal equipment (DTE) port.*

data rate. The rate at which data is transmitted or received from a device. Interactive applications tend to require a high data rate, while batch applications can usually tolerate lower data rates.

CPMI - CORREIOS
1346
Fls. Nº
Doc: 3690

data terminal equipment (DTE) port. A port that is capable of interfacing to a transmission circuit through a connection to a data communications equipment (DCE) port. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2 in a 9-pin connector (reversed in 25-pin connectors). See also *data communications equipment (DCE) port*.

DB-9 connector. A 9-pin version of the RS-232C port interface.

DCC. A dc converter.

DCE port. See *data communications equipment (DCE) port*.

DDR. Double data rate. See *data rate*.

defined zone configuration. The complete set of all zone objects that are defined in the fabric. The defined configuration can include multiple zone configurations. See also *enabled zone configuration* and *zone configuration*.

device. Hosts and storage that connect to a switch. Example devices are servers, redundant array of independent disks (RAID) arrays, and tape subsystems.

device connection controls. Enables organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by a worldwide name (WWN) and typically represent host bus adapters (HBAs) (servers). See also *access control lists*.

DID. The 3-byte destination ID of the destination device, in the 0xDomainAreaALPA format.

direct memory access (DMA). The transfer of data between memory and an input/output device without processor intervention.

disparity. The relationship of ones and zeros in an encoded character. *Neutral disparity* means an equal number of each, *positive disparity* means a majority of ones, and *negative disparity* means a majority of zeros.

DLS. See *dynamic load sharing*.

DMA. See *direct memory access*.

DNS. Distributed name server.

domain_ID. Unique identifier for the switch in a fabric. Usually automatically assigned by the switch, but can also be assigned manually. Can be any value between 1- 239.

DRAM. See *dynamic random access memory*.

DTE port. See *data terminal equipment (DTE) port*.

dual fabric. Two identical fabrics that allow redundancy in the event that one fabric fails. Use a dual fabric for mission critical applications.

dual-fabric SAN. A storage area network (SAN) that is composed of two independent fabrics. Synonymous with multi-fabric SAN. The two-fabric architecture makes dual-fabric SANs redundant.

DWDM. Dense wavelength digital multiplexing.

dynamic load sharing (DLS). Dynamic distribution of traffic over available paths. Allows for recomputing of routes when a fabric port or fabric loop port (Fx_port) or expansion port (E_port) changes status.

dynamic random access memory (DRAM). A storage in which the cells require repetitive application of control signals to retain stored data.

edge fabric. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric. See also *resilient core*.

edge switch. A switch whose main task is to connect nodes into the fabric. See also *core switch*.

E_D_TOV. See *error detect timeout value*.

EE_credit. See *end-to-end credit*.

effective zone configuration. The particular zone configuration that is currently in effect. Only one configuration can be in effect at once. The effective configuration is built each time a zone configuration is enabled.

EIA. Electronic Industry Association.

EIA rack. A storage rack that meets the standards set by the Electronics Industry Association (EIA).

electromagnetic compatibility (EMC). The design and test of products to meet legal and corporate specifications dealing with the emissions and susceptibility to frequencies in the radio spectrum. Electromagnetic compatibility is the ability of various electronic equipment to operate properly in the intended electromagnetic environment.

electromagnetic interference (EMI). Waves of electromagnetic radiation, including but not limited to radio frequencies, generated by the flow of electric current.

electrostatic discharge (ESD). The flow of current that results when objects having a static charge come into close enough proximity to discharge.

ELP. Extended link parameters.

ELWL. See *extra long wavelength*.

EMC. See *electromagnetic compatibility*.

EMI. See *electromagnetic interference*.

enabled zone configuration. The currently enabled configuration of zones. Only one configuration can be enabled at a time. See also *defined zone configuration* and *zone configuration.*

end port. A port on an edge switch that connects a device to the fabric.

end-to-end credit (EE_credit). The number of receive buffers allocated by a recipient port to an originating port. Used by class 1 and class 2 services to manage the exchange of frames across the fabric between source and destination. See also *end-to-end flow control* and *buffer-to-buffer credit.*

end-to-end flow control. Governs flow of class 1 and class 2 frames between node ports (N_ports). See also *end-to-end credit.*

E_port. See *expansion port.*

error. As applies to fibre channel, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors). See also *loop failure.*

error detect timeout value (E_D_TOV). The time that the switch waits for an expected response before declaring an error condition. Adjustable in 1 microsecond increments from 2 - 10 seconds.

ESD. See *electrostatic discharge.*

exchange. The highest level Fibre Channel mechanism used for communication between node ports (N_ports). Composed of one or more related sequences, and can work in either one or both directions.

expansion port (E_port). A port is designated an expansion port (E_port) when it is used as an inter-switch expansion port to connect to the E_port of another switch, to build a larger switch fabric.

Extended Fabrics. A feature that runs on Fabric operating system (OS) and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 km (62.14 mi).

extra long wavelength (ELWL). Laser light with a periodic length greater than 1300 nm (for example, 1420 or 1550). ELWL lasers are used to transmit Fibre Channel data over distances greater than 10 km. Also known as XLWL.

fabric. A network that uses high-speed fibre connections to connect switches, hosts, and devices. A fabric is an active, intelligent, nonshared interconnect scheme for nodes.

Fabric Access. Allows the application to control the fabric directly for functions such as discovery, access (zoning) management, performance, and switch control. Consists of a host-based library that interfaces the application to switches in the fabric over an out-of-band TCP/IP connection or in-band using an IP-capable host bus adapter (HBA).

Fabric Assist. A feature that enables private and public hosts to access public targets anywhere on the fabric, provided they are in the same Fabric Assist zone.

fabric configuration server (FCS) switch. One or more designated switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by worldwide name (WWN), and the list of designated switches is communicated fabric-wide. See also *backup FCS switch*, *primary FCS switch.*

fabric login (FLOGI). The process by which a device gains access to the fabric.

fabric loop port (FL_port). A fabric port that is loop capable. Used to connect node loop ports (NL_ports) to the switch in a loop configuration.

Fabric Manager. A feature that allows the storage area network (SAN) manager to monitor key fabric and switch elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values or counters and provides notification when defined boundaries are exceeded. The SAN manager can configure which elements, such as error, status, and performance counters, are monitored within a switch.

fabric mode. One of the modes for a loop port (L_port). An L_port is in fabric mode when it is connected to a port that is not loop capable and is using fabric protocol. See also *loop port* and *loop mode.*

fabric name. The unique identifier assigned to a fabric and communicated during login and port discovery.

Fabric OS. An operating system made up of two software components: the firmware that initializes and manages the switch hardware, and diagnostics.

fabric port (F_port). A port that is able to transmit under fabric protocol and interface over links. Can be used to connect a node port (N_port) to a switch. See also *fabric loop port* and *Fx_port.*

Fabric Watch. A feature that runs on Fabric operating system (OS) and allows monitoring and configuration of fabric and switch elements.

failover. The act that causes control to pass from one redundant unit to another.

FAN. Fabric address notification.

FC. See *fibre channel.*

FCA. See *Fibre Channel arbitrated loop.*

FC-AL. See *Fibre Channel arbitrated loop.*

RQS nº 03/2005 - CN - CPMI - CORREIOS
1347
Fls. Nº
3690
Doc:

FC-AL-3. The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCC. Federal Communications Commission.

FC-FLA. The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCMGMT. Fibre Alliance Fibre Channel Management.

FCP. See *Fibre Channel protocol.*

FC-PDLA. The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FC-PH-1,2,3. The Fibre Channel Physical and Signaling Interface standards defined by ANSI.

FC-PI. The Fibre Channel Physical Interface standard defined by ANSI.

FCS switch. See *fabric configuration server switch.*

FC-SW-2. The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches in order to create a multiswitch Fibre Channel fabric.

fibre channel (FC). A technology for transmitting data between computer devices at a data rate of up to 4 Gbps. It is especially suited for attaching computer servers to shared storage devices and for interconnecting storage controllers and drives.

Fibre Channel arbitrated loop (FC-AL). A standard defined on top of the FC-PH standard. It defines the arbitration on a loop where several FC nodes share a common medium.

Fibre Channel protocol (FCP). The protocol for transmitting commands, data, and status using Fibre Channel FC-FS exchanges and information units. Fibre channel is a high-speed serial architecture that allows either optical or electrical connections at data rates from 265 Mbps up to 4-Gbps.

Fibre Channel service (FS). A service that is defined by Fibre Channel standards and exists at a well-known address. For example, the Simple Name Server is a Fibre Channel service. See also *Fibre Channel service protocol.*

Fibre Channel service protocol (FSP). The common protocol for all fabric services, transparent to the fabric type or topology. See also *Fibre Channel service.*

Fibre Channel shortest path first (FSPF). A routing protocol used by Fibre Channel switches.

Fibre Channel transport. A protocol service that supports communication between Fibre Channel service providers. See also *Fibre Channel service protocol.*

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit can contain other field replaceable units.

File Transfer protocol (FTP). In Transmission Control protocol/Internet protocol (TCP/IP), an application protocol used for transferring files to and from host computers.

fill word. An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

firmware. The basic operating system provided with the hardware.

FLA. Fabric loop attach.

flash partition. Two redundant usable areas, called *partitions* into which firmware can be downloaded in the 2109 Model M12.

FLOGI. See *fabric login.*

FL_port. See *fabric loop port.*

F_port. See *fabric port.*

frame. The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, the data payload, a cyclic redundancy check (CRC), and an end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements, and so on) and data frames.

frame delimiter. A part of an ordered set that marks frame boundaries and describes frame contents. See also *ordered set.*

FRU. See *field replaceable unit.*

FS. See *Fibre Channel service.*

FSP. See *Fibre Channel service protocol.*

FSPF. See *Fibre Channel shortest path first.*

FTP. See *File Transfer protocol.*

full duplex. A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *half duplex.*

Fx_port. A fabric port that can operate as either a fabric port (F_port) or fabric loop port (FL_port). See also *fabric port* and *fabric loop port.*

gateway. Hardware that connects incompatible networks by providing the necessary translation for both hardware and software.

GBIC. See *gigabit interface converter.*

Gbps. Gigabits per second.

GBps. Gigabytes per second.

generic port (G_port). A generic port that can operate as either an expansion port (E_port) or a fabric port (F_port). A port is defined as a G_port when it is not yet connected or has not yet assumed a specific function in the fabric.

gigabit interface converter (GBIC). A removable serial transceiver module designed to provide gigabaud capability for fibre channel (FC) and other products that use the same physical layer.

gigabit switch. A 16-port, Fibre Channel gigabit switch.

G_port. See *generic port.*

half duplex. A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time). See also *full duplex.*

hard address. The arbitrated loop physical address (AL_PA) that a node loop port (NL_port) attempts to acquire during loop initialization.

hardware translative mode. Method for achieving address translation. The two hardware translative modes that are available to a QuickLoop-enabled switch are standard translative mode and QuickLoop mode. See also *standard translative mode* and *QuickLoop mode.*

HBA. See *host bus adapter.*

heartbeat. Through clustering software, the application server continually communicates with the clustered spare using network heartbeats to indicate to the other machines that everything is operating correctly. This heartbeat is typically carried over a dedicated network for clustering traffic. In cases of a problem (for example, a software crash on the operational server or a hardware component failure), a heartbeat link indicates to the other server that something has failed or is otherwise inoperative. If that heartbeat is lost, the spare server takes over the function provided by the application service. Depending on the clustering software, either the entire server or only specific services on the server can be failed over or failed back.

high availability. An attribute of the switch that identifies it as being capable of operating well in excess of 99 percent of the time. High Availability is typically identified by the number of nines in that percentage. For example, a switch that is rated at five nines would be capable of operating 99.999 percent of the time without failure.

high port count fabric. A fabric containing 100 or more ports.

host bus adapter (HBA). The interface card between a server or workstation bus and the Fibre Channel network.

hot pluggable. A field replaceable unit (FRU) capability that indicates it can be extracted or installed while customer data is otherwise flowing in the chassis.

hub. A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

IC bus. A serial, 2-wire bus used to monitor field replaceable unit (FRU) temperatures and control the system including blade power control.

ID. Identification.

IDB. Interface descriptor block.

IDLE. Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

IEC. International Electrotechnical Commission.

IETF. Internet Engineering Task Force.

information unit (IU). A set of information as defined by either upper-level process protocol definition or upper-lever protocol mapping.

initiator. A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *target.*

in-order delivery (IOD). A parameter that, when set, guarantees that frames are either delivered in order or dropped.

integrated fabric. The fabric created by six switches cabled together and configured to handle traffic as a seamless group.

Internet protocol (IP). In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

inter-switch link (ISL). A Fibre Channel link that connects two switches (a link from the expansion port (E_port) of one switch to the E_port of another).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1348
Fls. Nº
3690
Doc:

IOD. See *in-order delivery.*

IP. See *internet protocol.*

IPA. Initial process associator.

ISL. See *inter-switch link.*

ISL Trunking. A feature that enables distribution of traffic over the combined bandwidth of up to four inter-switch links (ISLs) (between adjacent switches), while preserving in-order delivery. A set of trunked ISLs is called a trunking group; each port employed in a trunking group is called a trunking port. See also *master port.*

isolated E_port. An expansion port (E_port) that is online but not operational between switches due to overlapping domain ID or nonidentical parameters such as error delay timeout values (E_D_TOVs). See also *expansion port.*

IU. See *information unit.*

K28.5. A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern. See also *comma.*

kernel flash. Flash memory that stores the bootable kernel code and is visible within the memory space of the processor. Data is stored as raw bits.

key pair. In public key cryptography, a pair of keys consisting of a public and private key of an entity. The public key can be publicized, but the private key must be kept secret.

LAN. See *local area network.*

latency. The period of time required to transmit a frame, from the time it is sent until it arrives.

LED. See *light-emitting diode.*

light-emitting diode (LED). A semiconductor chip that gives off visible or infrared light when activated.

link. As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibers. See also *circuit.*

link services. A protocol for link-related services.

LIP. See *loop initialization primitive.*

LM_TOV. See *loop master timeout value.*

local area network (LAN). A computer network located on a user's premises within a limited geographical area. (T)

logical unit number (LUN). An identifier used on a small computer systems interface (SCSI) bus to distinguish among up to eight devices (logical units) with the same SCSI ID.

long wavelength (LWL). A type of fiber optic cabling that is based on 1300 mm lasers and supports link speeds of 1.0625 Gbps. Can also refer to the type of GBIC or SFP. See also *short wavelength.*

loop. A configuration of devices that are connected to the fabric by way of a fabric loop port (FL_port) interface card.

loop circuit. A temporary bidirectional communication path established between loop ports (L_ports).

loop failure. Loss of signal within a loop for any period of time, or loss of synchronization for longer than the timeout value.

loop_ID. A hexadecimal value representing one of the 127 possible arbitrated loop physical address (AL_PA) values in an arbitrated loop.

loop initialization. The logical procedure used by a loop port (L_port) to discover its environment. Can be used to assign arbitrated loop physical address (AL_PA) addresses, detect loop failure, or reset a node.

loop initialization primitive (LIP). The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

looplet. A set of devices connected in a loop to a port that is a member of another loop.

loop master timeout value (LM_TOV). The minimum time that the loop master waits for a loop initialization sequence to return.

loop mode. One of the modes for a loop port (L_port). An L_port is in loop mode when it is in an arbitrated loop and is using loop protocol. An L_port in loop mode can also be in participating mode or nonparticipating mode. See also *loop port*, *fabric mode*, *participating mode*, and *nonparticipating mode.*

loop port (L_port). A node port (NL_port) or fabric port (FL_port) that has arbitrated loop capabilities. An L_port can be either in fabric mode or loop mode. See also *fabric mode* , *loop mode, nonparticipating mode,* and *participating mode.*

loop port state machine (LPSM). The logical entity that performs arbitrated loop protocols and defines the behavior of loop ports (L_ports) when they require access to an arbitrated loop.

L_port. See *loop port.*

LPSM. See *loop port state machine.*

LSR. Link state record.

LSU. Link state update.

LUN. See *logical unit number.*

LWL. See *long wavelength.*

MAC. Media access controller.

management information base (MIB). A simple network management protocol (SNMP) structure to help with device management, providing configuration and device information.

master port. As relates to trunking, the port that determines the routing paths for all traffic flowing through the trunking group. One of the ports in the first inter-switch link (ISL) in the trunking group is designated as the master port for that group. See also *ISL Trunking.*

MIB. See *management information base.*

modem serial port. The upper serial port on the control processor card (CP card) of the 2109 Model M12. Can be used to connect the CP card to a modem with a standard 9-pin modem cable. Consists of a DB-9 connector wired as an RS-232 device, and can be connected by serial cable to a data communications equipment (DCE) device. A Hayes-compatible modem or Hayes-emulation is required. The device name is ttyS1. See also *data communications equipment port* and *terminal serial port.*

multicast. The transmission of data from a single source to multiple specified node ports (N_ports), as opposed to all the ports on the network. See also *broadcast* and *unicast.*

multimode. A fiber optic cabling specification that allows up to 500 m (1640.5 ft) between devices.

name server. Frequently used to indicate Simple Name Server. See also *simple name server.*

NEMA. National Electrical Manufacturers Association.

NL_port. See *node loop port.*

NMS. Network Management System.

node. A Fibre Channel device that contains a node port (N_port) or node loop port (NL_port).

node loop port (NL_port). A node port that is loop capable. Used to connect an equipment port to the fabric in a loop configuration through a fabric loop port (FL_port).

node name. The unique identifier for a node, communicated during login and port discovery.

node port (N_port). A node port that is not loop capable. Used to connect an equipment port to the fabric.

nonparticipating mode. A mode in which a loop port (L_port) in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an arbitrated loop physical address (AL_PA) cannot be acquired. See also *participating mode.*

nonvolatile random access memory (NVRAM). Random access memory (storage) that retains its contents after the electrical power to the machine is shut off. A specific part of NVRAM is set aside for use by the system ROS for the boot device list.

N_port. See *node port.*

NVRAM. See *nonvolatile random access memory.*

Nx_port. A node port that can operate as either a node port (N_port) or node loop port (NL_port). See also *node port* and *node loop port.*

operating system (OS). A collection of system programs that control the overall operation of a computer system.

ordered set. A transmission word that uses 8b/10b mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include frame delimiters, primitive signals, and primitive sequences. Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames. See also *frame delimiter*, *primitive signal*, and *primitive sequence.*

OS. See *operating system.*

packet. A set of information transmitted across a network. See also *frame.*

participating mode. A mode in which a loop port (L_port) in a loop has a valid arbitrated loop physical address (AL_PA) and can arbitrate, send frames, and retransmit received transmissions. See also *nonparticipating mode.*

path selection. The selection of a transmission path through the fabric. Switches use the Fibre Channel shortest path first (FSPF) protocol.

PCI. Peripheral control interconnect.

PDU. Power distribution unit.

Performance Monitoring. A feature that provides error and performance information to the administrator and user for use in storage management.

phantom address. An arbitrated loop physical address (AL_PA) value that is assigned to a device that is not physically in the loop. Also known as phantom AL_PA.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1349
Fls. Nº
3690
Doc:

phantom device. A device that is not physically in an arbitrated loop, but is logically included through the use of a phantom address.

PLDA. See *private loop direct attach.*

PLOGI. See *port login.*

PMC. PCI mezzanine card.

P/N. Part number.

point-to-point. A Fibre Channel topology that employs direct links between each pair of communicating entities.

port cage. The metal casing extending out of the optical port on the switch, and in which the gigabit interface converter (GBIC) or small form-factor pluggable (SFP) can be inserted.

port card. A Fibre Channel card that contains optical or copper port interfaces, and acts like a switch module. See also *16-port card.*

port login (PLOGI). The port-to-port login process by which initiators establish sessions with targets. See also *fabric login.*

port module. A collection of ports in a switch.

port_name. The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST. See *power-on self-test.*

power-on self-test (POST). A series of diagnostics that are automatically run by a device when the power is turned on.

primary FCS switch. Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric. See also *backup FCS switch* and *FCS switch.*

primitive sequence. A part of an ordered set that indicates or initiates port states. See also *ordered set.*

primitive signal. A part of an ordered set that indicates events. See also *ordered set.*

principal switch. The switch that assumes the responsibility to assign domain IDs. The role of principal switch is negotiated after a "build fabric" event.

private device. A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.

private loop. An arbitrated loop that does not include a participating fabric loop port (FL_port).

private loop direct attach (PLDA). A subset of fibre channel standards for the operation of peripheral devices.

private NL_port. A node loop port (NL_port) that communicates only with other private NL_ports in the same loop and does not log into the fabric.

protocol. A defined method and a set of standards for communication.

public device. A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

public loop. An arbitrated loop that includes a participating fabric loop port (FL_port), and can contain both public and private node loop ports (NL_ports).

public NL_port. A node loop port (NL_port) that logs into the fabric, can function within either a public or private loop, and can communicate with either private or public NL_ports.

quad. A group of four adjacent ports that share a common pool of frame buffers.

QuickLoop. (1) A feature that makes it possible to allow private devices within loops to communicate with public and private devices across the fabric through the creation of a larger loop. (2) The arbitrated loop created using this software. A QuickLoop can contain a number of devices or looplets; all devices in the same QuickLoop share a single arbitrated loop physical address (AL_PA) space.

QuickLoop mode. A hardware translative mode that allows private devices to communicate with other private devices across the fabric. See also *hardware translative mode* and *standard translative mode.*

RAID. See *redundant array of independent disks.*

RAM. See *random access memory.*

RAN. Remote Asynchronous Notification.

random access memory (RAM). A temporary storage location in which the central processing unit (CPU) stores and executes its processes.

R_A_TOV. See *resource allocation timeout value.*

read only memory (ROM). Memory in which stored data cannot be changed by the user except under special conditions.

receiver ready (R_RDY). A primitive signal indicating that the port is ready to receive a frame.

reduced instruction set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid processing.

redundant array of independent disks (RAID). A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

registered state change notification (RSCN). A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

remote fabric. A fabric that spans across wide area networks (WANs) by using protocol translation (a process also known as tunneling) such as fibre channel over asynchronous transfer mode (ATM) or fibre channel over Internet protocol (IP).

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server.

Remote Switch. A feature that runs on Fabric operating system (OS) and enables two fabric switches to be connected over an asynchronous transfer mode (ATM) connection. This requires a compatible Fibre Channel to ATM gateway, and can have a distance of up to 10 km (6.214 mi) between each switch and the respective ATM gateway.

request rate. The rate at which requests arrive at a servicing entity. See also *service rate*.

resilient core. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric.

resource allocation timeout value (R_A_TOV). Used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. This value is adjustable in one microsecond increments from 10 - 120 seconds.

resource recover timeout value (RR_TOV). The minimum time a target device in a loop waits after a loop initialization primitive (LIP) before logging out a small computer systems interface (SCSI) initiator. See also *error detect timeout value* and *resource allocation timeout value*.

RISC. See *reduced instruction set computer*.

RLS probing. Read link status of the arbitrated loop physical addresses (AL_PAs).

ro. Read only.

ROM. See *read only memory*.

route. As applies to a fabric, the communication path between two switches. Can also apply to the specific path taken by an individual frame, from source to destination. See also *Fibre Channel shortest path first*.

routing. The assignment of frames to specific switch ports, according to frame destination.

RPC. See *remote procedure call*.

R_RDY. See *receiver ready*.

RR_TOV. See *resource recovery timeout value*.

RS-232 port. A port that conforms to a set of Electrical Industries Association (EIA) standards. Used to connect data terminal equipment (DTE) and data communications equipment (DCE) devices for communication between components, terminals, and modems. See also *DB-9 connector*, *DCE port*, and *DTE port*.

RSCN. See *registered state change notification*.

RSH. Remote shell.

RTC. Real time clock.

rw. Read-write.

SAN. See *storage area network*.

SAN island. A group of storage devices and servers connected to switches in a fabric.

SC. Standard connector.

SCSI. See *small computer systems interface*.

SCSI Enclosure Services (SES). A subset of the small computer systems interface (SCSI) protocol used to monitor temperature, power, and fan status for enclosure devices.

SDRAM. See *synchronous dynamic random access memory*.

Secure Fabric OS. An optionally-licensed software product that runs on top of the Fabric OS and provides customizable security restrictions through local and remote management channels on a switch.

secure sockets layer (SSL). A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

sequence. A group of related frames transmitted in the same direction between two node ports (N_ports).

SERDES. Serializer/deserializer.

service rate. The rate at which an entity can service requests. See also *request rate*.

SES. See *SCSI Enclosure Services*.

SFP. See *small form-factor pluggable*.

short wavelength (SWL). A type of fiber optic cabling that is based on 850 mm lasers and supports 1.0625 Gbps link speeds. Can also refer to the type of gigabit

CPMI - CORREIOS
1350
Fls Nº
3690
Doc:

interface converter (GBIC) or small form-factor pluggable (SFP). See also *long wavelength*.

SID. The 3-byte source ID of the originator device, in the 0xDomainAreaALPA format.

SID-DID. Source identifier-destination identifier.

SIMMS. Single in-line modules.

simple name server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Can also be referred to as directory service. See also *Fibre Channel service*.

simple network management protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

single mode. The fiber optic cabling standard that corresponds to distances of up to 10 km (6.214 mi) between devices.

small computer systems interface (SCSI). A parallel bus architecture and a protocol for transmitting large data blocks up to a distance of 15 - 25 m (49 - 82 ft).

small form-factor pluggable (SFP). An optical transceiver used to convert signals between optical fiber cables and switches.

SMI. Special memory interface.

SNIA. Storage Network Industry Association.

SNMP. See *simple network management protocol*.

SNMPv1. The original standard for SNMP, now labeled v1.

SNS. See *simple name server*.

SOF. Start-of-frame.

SSL. See *secure sockets layer*.

standard translative mode. A hardware translative mode that allows public devices to communicate with private devices across the fabric. See also *hardware translative mode* and *QuickLoop mode*.

storage area network (SAN). A network of systems and storage devices that communicate using Fibre Channel protocols. See also *fabric*.

subordinate switch. All switches in the fabric other than the principal switch. See also *principal switch*.

switch. Hardware that routes frames according to Fibre Channel protocol and is controlled by software.

switch name. The arbitrary name assigned to a switch.

switch port. A port on a switch. Switch ports can be expansion ports (E_ports), fabric ports (F_ports), or fabric loop ports (FL_ports).

SWL. See *short wavelength*.

synchronous dynamic random access memory (SDRAM). The main memory for the switch. Used for volatile storage during switch operation.

Tachyon. A type of host bus adapter.

target. A storage device on a Fibre Channel network. See also *initiator*.

TCP. See *transmission control protocol*.

tenancy. The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

terminal serial port. The lower serial port on the control processor card (CP card) of the 2109 Model M12. This port sends switch information messages and can receive commands. Can be used to connect the CP card to a computer terminal. Has an RS-232 connector wired as a data terminal equipment (DTE) device, and can be connected by serial cable to a data communications equipment (DCE) device. The connector pins 2 and 3 are swapped so that a straight-through cable can be used to connect to a terminal. The device name is ttyS0. Can also be referred to as the console port. See also *DCE port, DTE port,* and *modem serial port*.

throughput. The rate of data flow achieved within a cable, link, or system. Usually measured in bits per second (bps). See also *bandwidth*.

topology. As applies to fibre channel, the configuration of the Fibre Channel network and the resulting communication paths allowed.

translative mode. A mode in which private devices can communicate with public devices across the fabric.

transmission character. A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Control protocol (TCP). A communications protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for Internet protocol.

transmission word. A group of four transmission characters.

trap (SNMP). The message sent by a simple network management protocol (SNMP) agent to inform the SNMP management station of a critical error. See also *simple network management protocol.*

tunneling. A technique for enabling two networks to treat a transport network as though it were a single communication link or local area network (LAN).

Tx. Transmitted.

U. Unit of measure for rack-mounted equipment.

UART. Universal Asynchronous Receiver Transmitter.

UDP. See *user datagram protocol.*

ULP. See *upper-level protocol.*

ULP_TOV. See *upper-level timeout value.*

unicast. The transmission of data from a single source to a single destination. See also *broadcast* and *multicast.*

universal port (U_port). A switch port that can operate as a generic port (G_port), expansion port (E_port), fabric port (F_port), or fabric loop port (FL_port). A port is defined as a U_port when it is not connected or has not yet assumed a specific function in the fabric.

U_port. See *universal port.*

upper-level protocol (ULP). The protocol that runs on top of Fibre Channel. Typical upper-level protocols are small computer system interface (SCSI), Internet protocol (IP), HIPPI, and IPI.

upper-level timeout value (ULP_TOV). The minimum time that a small computer system interface (SCSI) upper-level protocol (ULP) process waits for SCSI status before initiating ULP recovery.

user datagram protocol (UDP). A protocol that runs on top of Internet protocol (IP) and provides port multiplexing for upper-level protocols.

user flash. See *compact flash.*

VC. See *virtual circuit.*

VCCI. Voluntary Control Council for Interference

virtual circuit (VC). A one-way path between node ports (N_ports) that allows fractional bandwidth.

WAN. See *wide area network.*

WDM. Wave division multiplexing.

well-known address. As pertaining to fibre channel, a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan network, and that can use or provide public communications facilities. (T)

workstation. A computer used to access and manage the fabric. Can also be referred to as a management station or host.

worldwide name (WWN). Uniquely identifies a switch on local and global networks.

World Wide Web (WWW). A network of servers that contain programs and files. Many of the files contain hypertext links to other documents available through the network.

WWN. See *worldwide name.*

WWW. See *World Wide Web.*

XLWL. See *extra long wavelength.*

zone. A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone. See also *zoning.*

zone alias. An alias for a set of port numbers or worldwide names (WWNs). Zone aliases can be used to simplify the entry of port numbers and WWNs. For example, "host" could be used as an alias for a WWN of 110:00:00:60:69:00:00:8a.

zone configuration. A set of zones designated as belonging to the same zone configuration. When a zone configuration is in effect, all valid zones in that configuration are also in effect.

zone member. A port, node, worldwide name (WWN), or alias, which is part of a zone.

zone scheme. The level of zoning granularity selected. For example, zoning can be done by switch or port, worldwide name (WWN), arbitrated loop physical address (AL_PA), or a mixture. See also *zone configuration.*

zone set. See *zone configuration.*

Zoning. A feature that runs on Fabric operating system (OS) and allows partitioning of the fabric into logical groupings of devices. Devices in a zone can only access and be accessed by devices in the same zone. See also *zone.*

RQS nº 03/2005 - CN - CPMI - CORREIOS
FLS. Nº 1351
Doc: 3690

Index

Numerics

16-port card
  description 28
  LEDs 32
  removing 70
  replacing 74
  specifications 100
2109 Model C36
  attaching
    concrete floor 10
    concrete floor beneath a raised floor 12
    front door 16
    mounting plates 15
    stabilizers 9
  checking
    customer's ac power source 16
    power distribution unit 17
  connecting the switch and device cables 18
  installing 7
  leveling 8
  positioning 7
  powering on the cabinet 18
  regulatory specifications 107
  with Model M12 library xxiii
2109 Model M12
  16-port card 28
  ac power input connectors and ac power switches 30
  blower assembly
    description 30
    side 4
  cable management items 31
  circuit breaker 30
  components 27, 99
  control processor cards 28
  diagnostic tests 43
  features 1
  field replaceable units (FRUs) 43
  installing
    additional model 51
    modems 45, 47
  interpreting
    LED activity 32
    POST 42
  LEDs
    16-port card 32
    blower assembly 40
    CP card 35
    power supply 38
    WWN card 31, 41
  maintenance commands and environmental status 44
  management interfaces 5
  managing and monitoring 4
  operating 27
  overview 1
  parts 117
2109 Model M12 *(continued)*
  port side 3
  power supplies 30
  removing additional model 51
  setting up a remote modem system 46
  standard shipment 53
  starting and configuring 19
  turning on and off 27
  unpacking 53
  verifying modem installation 48
24-inch load plate
  part number 52
  using 60

A

about this document xxiii
ac grounding check xviii
ac power
  external cords 17
  how to remove xiv
  input connectors 30
  switches 30
ac power distribution unit
  power-off procedure 70
  power-on procedure 69
  removing 95
  replacing 95
accessory kit 53
activity LED, interpreting 32
address of IBM xxv
Advanced Security feature 2
Agency Certification label xii
assembly, blower
  description 30
  LEDs 40
  side of chassis 4
attaching
  cabinet to concrete floor 10, 12
  front door 16
  mounting plate 15
  stabilizer 9
attention notices xi
audience xxiii

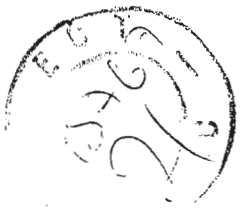
B

battery
  CP card 99
  CP card, replacing 86
  notice, caution xxii
  specifications 101
bezel
  description 31
  LEDs 41
blank
  fillers 111

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1252
Doc: 3690

blank *(continued)*
planning worksheets 119
blower assembly
description 30
LEDs 40
removing 90
replacing 90
side of chassis 4
time required 90
brace, earthquake 110
brackets, installing 55
bridge tool
alignment label, inspecting xviii
inspecting the label xviii
ordering 52
part number 52
purpose of 52
returning 52
using 60
Brocade
documents xxiii
IBM product and model number matrix xxiv



C

cabinet
attaching to a concrete floor 10
attaching to concrete floor 12
door, removing and replacing 96
external check xiii
inspection xi
installing the 2109 Model M12 55
leveling 8
parts 115
positioning 7
power on 18
power-off procedure 70
power-on procedure 69
relocating 97
removing a 2109 Model M12 from 65
removing and replacing the PDU 94
safety label checks xii
service 69
cable management
items 31
tray
removing 91
replacing 92
cables
alignment 25
guides 32
recommendations for managing 75
card
16-port card 28
control processor 28
WWN 31
caution notices
battery xxii
definition xi
chassis
port side 3
chassis *(continued)*
providing initial power 19
chassis door
removing 54, 96
replacing 96
check
ac grounding xviii
ac power source of the customer 16
ground xviii
machine, external xiv
machine, internal xiv
PDU 17
safety label xv
Chinese Class A compliance statement 124
circuit breaker 30
Class 1 laser product xxi
comments, how to send xxv
components
2109 Model M12 99
switch 27
concrete floor cabinet attachment 10, 12
conducting
external machine checks xiv
internal machine checks xiv
safety inspections xi
configuration
2109 Model M12 19
parameters 21
switch 21
Confirming, a failed CP card 76
connect the switch and device cables 18
control processor card
description 28
determining the status 29
LEDs 35
removing 79
replacing 81
specifications 101
cords, power 113
covers, parts 109
CP card battery, replacing 86
customer ac power source 16

D

danger notices xi
device cables, connecting 18
diagnostic tests 43
digital meter xviii
dimensions, physical 99
director of licensing, address 123
disposal, product xxii
Do Not Operate tag 16
document, about this xxiii
door
cabinet
removing 96
replacing 97
chassis
removing 54, 96
replacing 96

E

earthquake brace, parts 110
edition notice ii
electrical safety 69
electronic emission statements 124
environmental
  notices and statements xxi
  requirements 104
  status and maintenance commands 44
Ethernet port 29
European Community compliance statement 125
Extended Fabrics 2
external
  ac power cords 17
  cabinet checks xiii
  machine checks
    battery notice caution xxii
    how to conduct xiv

F

Fabric Manager 2
facility specifications 103
factory, configuration 18
FCC
  emission limits 124
  rules 124
  statement 124
  unauthorized changes or modifications 124
FDA 21 CFR 1040.10 and 1040.11 xxi
features
  Advanced Zoning 2
  Fabric Watch 2
  ISL Trunking 2
  Performance Monitoring 2
  software
    Advanced Security 2
    Extended Fabrics 2
    Fabric Manager 2
    Remote Switch 2
  Web Tools 2
features, 2109 Model M12 1
Federal Communications Commission (FCC) statement 124
Fibre Channel Association Web site xxiv
Fibre Channel port specifications 102
field replaceable units (FRUs) 43
filler panel
  16-port card, removing 70
  16-port card, replacing 74
  CP card, removing 79
  CP card, replacing 81
  power supply, removing 87
  power supply, replacing 89
fire suppression systems xxii
form
  non-IBM alteration attachment survey xiv
  reader comment, how to send xxv
front door attachment 16
fruinfoset command 97
fusing caution label xvi

G

general specifications of the 2109 Model C36 with Model M12 105
genie tool and load plate label, inspecting xviii
Germany compliance statement 125
getting
  help xxiv
  software updates xxiv
ground
  attachment plug 17
  checking ac xviii
  checks xviii
  lug xviii
guidelines
  safety 51

H

heavy load label xvi
help, getting xxiv
high
  leakage current label xii
  voltage, ac 17
High-availability feature 1
how to send your comments xxv

I

IBM
  address xxv
  notices 123
  trademarks 124
IBM product and model number matrix xxiv
IEC 825-1 xxi
in-band management method 4
Industry Canada compliance statement 124
information, parts 109
inlet, power requirements 103
inspection
  bridge tool xviii
  Model 2109 M12 switch xiv
  safety, cabinet xi
  safety, conducting xi
installation considerations and safety guidelines 51
installing
  2109 Model C36 7
  2109 Model M12 in the cabinet 55, 60
  additional 2109 Model M12 51
  brackets 55
  modems 45, 47
intellectual property 123
interference, radios and televisions 124
internal machine checks xiv
interpreting
  LED activity 32
  POST 42
items
  2109 Model M12 standard shipment 53

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1353
3690
Doc: Index 143

items *(continued)*
cable management 31
needed
configure and connect the 2109 Model M12 20
required
remove a blower assembly 90
remove a cable management tray 91

J

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 126

K

Korean Government Ministry of Communication (MOC) statement 126

L

label
Agency Certification xii
bridge tool alignment xviii
check, safety xv
fusing caution xvi
Genie tool and load plate xx
heavy load xvi
high leakage current danger xii
linecord caution xv
pinch point xxi
power supply cord caution xii
power supply cover caution xvi
SFP xvii
tilt warning xx
laser safety xxi
LEDs
16-port card 32
activity, interpreting 32
blower assembly 40
control processor card 35
patterns
16-port card 33
blower assembly 40
CP card 37
power supply 39
power supply 38
WWN card and bezel 41
leveling
cabinet 8, 14
feet 8, 113
license
for patents 123
lift tool
arbocrate (shipping container) 53
ordering procedure 52
part number 52
United States ordering procedure 52
unpacking, assembly and repacking 55
using 60, 65
World trade ordering procedure 52
linecord caution label xv
lug, ground xviii

M

machine checks
external xiv
internal xiv
maintaining the 2109 Model M12 43
maintenance commands and environmental status 44
managing
cable items 31
cables, recommendations 75
materials, recyclable xxii
memory specifications 101
meter, digital xviii
modem
installation, verifying 48
installing 45, 47
serial port port pinouts 102
serial port specifications 102
setup 46
monitoring and managing the switch 4
mounting plate attachment 15

N

needed items, to configure and connect the 2109 Model M12 20
non-IBM alteration attachment survey form xiv
notices
caution, battery xxii
environmental xi, xxi
IBM 123
safety xi, 69

O

operating the 2109 Model M12 27
optical port terminators xxi
ordering the lift tool and the 24–inch load plate 52
out-of-band management method 4
overview of the 2109 Model M12 1

P

parameters
configuration 21
modem for Windows 95, 98, 2000, ME or NT, or TERM in a UNIX environment 47
part number
24-inch load plate 52
lift tool 52
parts
2109 Model M12 117
blank fillers 111
covers 109
earthquake brace 110
information 109
leveling feet 113
PDU 116

parts *(continued)*
power cords 113
stabilizers 112
supplied with the 14U mount kit 115
patents 123
PDU
check 17
parts 116
power-off procedure 70
power-on procedure 69
removing 95
replacing 95
physical dimensions 99
pinch point label, inspecting xviii
pinouts
modem serial port 102
terminal serial port 101
planning worksheet 119
port
configuration worksheet 120
Ethernet 29
modem serial 29
side of chassis 3
switch 99
terminal serial 29
terminal serial, specifications 101
position the cabinet 7
POST
interpreting 42
restarting 107
specifications 107
power
cords
external 17
list of 113
removing xiv
source check 16
specifications 103
to the chassis 19
power distribution unit (PDU)
check 17
parts 116
power-off procedure 70
power-on procedure 69
removing 95
replacing 95
power supply
cord caution label xii
cover caution label xvi
description 30
LEDs 38
removing 87
replacing 89
turning on and off 27
power-off procedure
PDU 70
power-on procedure
cabinet 69
PDU 69
product
disposal xxii
product *(continued)*
recycling xxii
specifications 99, 100
proper grounding xviii
providing initial power to the chassis 19
publications
2109 Model C36 with Model M12 library xxiii
Web sites xxiv

R

radio interference 124
reader comment form processing xxv
recommendations for managing cables 75
Recording critical switch information 77
recycling products xxii
reference information for the fruinfoset command 97
regulatory specifications 106
related documents xxiii
relocating the cabinet 97
remote modem setup 46
Remote Switch 2
removing
16-port card 70
16-port card filler panel 70
2109 Model M12 from the cabinet 65
ac power xiv
blower assembly 90
cabinet door 96
cable management tray 91
chassis door 54, 96
CP card 79
filler panel 79, 87
PDU 94
power supply or filler panel 87
removing and replacing
16-port card 70
16-port card filler panel 70
blower assembly 89
cable management tray 91
chassis door 95
CP card or filler panel 75
front and rear doors 96
PDU 94
power supply or filler panel 86
WWN card 93
replacing
16-port card 74
16-port card filler panel 74
blower assembly 90
cabinet door 97
cable management tray 92
chassis door 96
CP card battery 86
CP card or filler panel 81
filler panel 81, 89
PDU 95
power supply or filler panel 89
required items
to remove a blower assembly 90
requirements, environmental 104

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Index 1354
Fls. Nº 345
Doc: 3690

restarting the switch 107
restrictions, usage xxi
running a POST 42

S

safety
  cabinet label check xii
  electrical 69
  external cabinet check xiii
  external machine checks xiv
  guidelines 51
  inspection, how to conduct xi
  internal machine checks xiv
  label check xv
  laser xi, xxi
  notices xi, 69
  product disposal xxii
sending your comments xxv
servicing the cabinet 69
setting up a remote modem system 46
SFP label xvii
software
  features
    Advanced Security 2
    Advanced Zoning 2
    Extended Fabrics 2
    Fabric Manager 2
    Fabric Watch 2
    ISL Trunking 2
    Performance Monitoring 2
    Remote Switch 2
    Web Tools 2
  getting updates xxiv
specifications
  16-port card 100
  battery 101
  facility 103
  Fibre Channel port 102
  general 105
  memory 101
  modem serial port 102
  POST 107
  power 103
  product 100
  regulatory 106
  restarting 107
  terminal serial port 101
SPF, inserting 25
stabilizer
  attaching 9
  parts 112
standard shipment items 53
starting and configuring the 2109 Model M12 19
statements
  Chinese Class A compliance 124
  electronic emission 124
  European Community compliance 125
  Federal Communications Commission 124
  Germany compliance 125
  Industry Canada compliance 124
statements *(continued)*
  Japanese Voluntary Control Council for Interference (VCCI) class 1 126
  Korean Government Ministry of Communication (MOC) 126
  Taiwan class A compliance 126
switch
  components 27, 99
  configuring 19, 21
  connecting 18
  inspecting the Model 2109 M12 xiv
  managing 4
  operating 27
  ports 99
  POST, interpreting 42
  restarting 42
  specifications
    facility 103
    general 105
    memory 101
    modem serial port 102
    power 103
    regulatory 106
    terminal serial port 101
  turning on and off 27
  worksheets
    planning 119
    port configuration 120
    zone configuration 122
    zone definition 121
systems, fire suppression xxii

T

tag, Do Not Operate tag 16
Taiwan class A compliance statement 126
take-back program, product xxii
terminal
  serial port specifications 101
terminators for optical ports xxi
tests, diagnostic 43
tie wraps 32
tilt warning label, inspecting xviii
time required to install the 2109 Model M12 in the cabinet 55
time required to remove and replace
  16-port card or filler panel 70
  blower assembly 90
  cable management tray 91
  chassis door 95
  CP card or filler panel 76
  power supply or filler panel 87
tools required to install the 2109 Model M12 in the cabinet 55
trademarks 124
turning on and off the 2109 Model M12 27

U

United States ordering procedure for the lift tool and the 24-inch load plate 52

units , field replaceable 43
unpacking the 2109 Model M12 53
updates, getting software xxiv
usage restrictions xxi
using the lift tool, the 24-inch load plate, and the bridge tool 60

V

verifying
  if the WWN card needs replacing 93
  modem installation 48
  the operation of the new CP card 82
voltage level at power source xviii

W

Web sites xxiv
weight, component 99
who should read this document xxiii
worksheets
  blank 119
  planning 119
  port configuration 120
  zone configuration 122
  zone definition 121
World trade ordering procedure for the lift tool and the 24-inch load plate 52
WWN card
  and bezel 31
  and bezel LEDs 41
  restarting the switch 31

Z

zone
  configuration worksheet 122
  definition worksheet 121

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1355
Doc: 3690

Readers' comments—we would like to hear from you

IBM TotalStorage SAN Cabinet
2109 Model C36 with Model M12
Installation and Service Guide

Publication No. GC26-7467-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

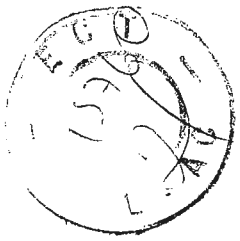
Phone No.

1356
CPMI - CORREIOS
Fls. Nº
3690

Readers' Comments — We'd Like to Hear from You
GC26-7467-03

IBM®

Cut or Fold
Along Line



Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
RCF Processing Department
M86/050-3
5600 Cottle Road
San Jose, CA 95193-0001

Fold and Tape | **Please do not staple** | Fold and Tape

GC26-7467-03

Cut or Fold
Along Line

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1357
Doc: 3690

Spine information:

IBM

IBM TotalStorage SAN Cabinet

IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12: Installation and Service Guide

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1388
Doc: 3699

Manual 04

Interoperability Matrix

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1359
Doc: 3690

IBM TotalStorage™ Enterprise Storage Server™

Interoperability Matrix

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1360
Doc: 3690

June 27, 2003

© Copyright International Business Machines Corporation 1999, 2002, 2003. All rights reserved.

The information provided in this document is provide "AS IS" without warranty of any kind, including any warranty of merchantability, fitness for a particular purpose, interoperability or compatibility. IBM's products are warranted in accordance with the agreements under which they are provided.

Unless otherwise specified, the product manufacturer, supplier, or publisher of non-IBM products provides warranty, service, and support directly to you. IBM makes no representations or warranties regarding non-IBM products.

The inclusion of an IBM or non-IBM product on an interoperability list is not a guarantee that it will work with the designated IBM storage product. In addition, not all software and hardware combinations created from compatible components will necessarily function properly together. The following list includes products developed or distributed by companies other than IBM. IBM does not provide service or support for the non-IBM products listed, but does not prohibit them from being used together with IBM's storage products. During problem debug and resolution, IBM may require that hardware or software additions be removed from the IBM product to provide problem determination and resolution on the IBM-supplied hardware/ software. For support issues regarding non-IBM products, please contact the manufacturer of the product directly. IBM does not warrant either functionality or problem resolution of any non-IBM products.

This information could include technical inaccuracies or typographical errors. IBM does not assume any liability for damages caused by such errors as this information is provided for convenience only; the reader should confirm any information contained h[illegible] with the associated vendor.

[illegible]anges are periodically made to the content of the document. These changes will be incorporated in new editions of the document. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this document at anytime without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

T[illegible]llowing terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AS/400	IBM logo	S/390
DYNIX	Micro Channel	S/390 Parallel Enterprise Server
DYNIX/ptx	Multiprise	SP
e (logo)	Netfinity	TotalStorage
Enterprise Storage Server	NUMA-Q	Versatile Storage Server
ESCON	OS/390	VM/ESA
ES/9000	OS/400	VSE/ESA
FICON	PTX	xSeries
FlashCopy	pSeries	z/OS
IBM	Redbooks	zSeries
	RS/6000	z/VM

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1361
Doc: 3690

CONTENTS

Introduction 2
ESS Interoperability Summary 3
Configuration Planning 4
ESS Copy Services 6
Data General Servers 9
Hewlett-Packard Servers – HP-UX 11
Hewlett-Packard Servers – OpenVMS 13
Hewlett-Packard Servers – Tru64 UNIX 15
IBM iSeries and AS/400 Servers 17
IBM NUMA-Q Servers 19
IBM pSeries and RS/6000 Servers 21
IBM RS/6000 SP Servers 25
IBM zSeries and S/390 Servers 29
Intel-based Servers – Linux 34
Intel-based Servers – NetWare 36
Intel-based Servers – Windows 39
SGI Servers 42
Sun Servers 44
Network Attached Storage (NAS) 47
Appendix A: ESS Host Adapters and Cables 49
Appendix B: Host Adapter Products 50
Appendix C: SAN Fabric Products 53
Appendix D: Revision History 54

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1362
Doc: 3690

INTRODUCTION

About this Document

This document lists interoperable environments and configurations for IBM TotalStorage Enterprise Storage Server (ESS).

The document is for informational and planning purposes only and may change at anytime. This version supersedes and replaces all previous versions. The latest version of this document is available at:

http://www.ibm.com/storage/hardsoft/products/ess/supserver.htm

Not all combinations created from interoperable components are supported, nor will they necessarily function properly together. The customer is responsible for confirming that a specific configuration (i.e. server model, operating system level, host adapter, and fabric product combination) is a valid and supported configuration by each of the vendors whose products are included in the configuration.

This document is not intended to be the sole resource for configuration information, requirements, and prerequisites. Refer to ESS publications, vendor documentation, or your IBM Sales Representative or IBM Business Partner for additional information.

End-of-Service / End-of-Support

Throughout this document, this symbol – @ – indicates that the product vendor has announced that they no longer provide support for the product. If problems are encountered with existing installations, you may be required to update your configuration to a supported level before problem determination can take place.

Request for Price Quotations (RPQ)

If a desired configuration is not represented in this document, a RPQ should be submitted to IBM to request approval. To submit a RPQ, contact your local IBM Storage Specialist or Business Partner.

Examples of configurations supported via RPQ are available at:

http://www.storage.ibm.com/hardsoft/products/ess/additional_config.html

What's New

This version is dated June 27, 2003 and has been updated as noted below. It replaces the version dated May 13, 2003. Unless stated otherwise, these items require ESS LIC level 2.2.0, or later.

Servers

- IBM BladeCenter (Intel(Linux and Windows))
- IBM TotalStorage SAN Volume Controller
- pSeries 615 Models 6C3 and 6E3

Operating Systems, Path Management, and Clustering

- UnitedLinux 1.0 (iSeries and pSeries): SuSE Enterprise Server 8
- Windows 2003 SDD
- zSeries: Added End-of-Service/End-of-Support notation for zSeries O/S levels
- zSeries Fibre Channel Protocol
- zSeries: z/VM Version 4 Release 3

Host Adapters

- Emulex LP9402DC and LP 9802: Added availability date for support on NetWare
- IBM FC 6239 (pSeries)
- SGI PCX-FC-2OPT-B

SAN Fabric

- IBM RS/6000: Cisco MDS 9216 and 9509

ROS nº 03/2005 - CN - CPMI - CORREIOS
1363
Fls. Nº
Doc: 3690

ESS INTEROPERABILITY SUMMARY

For convenience, the following tables summarize the interoperable environments and configurations for the ESS. Refer to the individual server pages for additional information, including prerequisites and limitations.

Table 1: Open Systems

	ESS Model 800	ESS Models F10 and F20	ESS Models E10 and E20	Fibre Channel	SCSI	Clustering (Fibre Channel)	Clustering (SCSI)	Boot device support	Subsystem Device Driver (SDD)	ESS Application Program Interface (ESS API)	ESS Command Line Interface (ESS CLI)	Copy Services Command Line Interface (ESS CLI)
Data General (DG/UX)		✓	✓		✓							
Hewlett-Packard (HP-UX)	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
Hewlett-Packard AlphaServer (OpenVMS)	✓	✓	✓	✓	✓	✓	✓					✓
Hewlett-Packard AlphaServer (Tru64 UNIX)	✓	✓	✓	✓	✓	✓	✓	✓				✓
IBM iSeries and AS/400 (OS/400)	✓	✓	✓	✓	✓							
IBM iSeries and AS/400 (Linux)	✓			✓								
IBM pSeries, RS/6000, and RS/6000 SP (AIX)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IBM NUMA-Q (DYNIX/ptx)	✓	✓	✓	✓		✓						✓
Intel Servers (Linux)	✓	✓		✓					✓	✓	✓	✓
Intel Servers (NetWare)	✓	✓	✓	✓	✓	✓	✓		✓			✓
Intel Servers (Windows)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SGI Origin Servers (IRIX)	✓	✓		✓								
Sun (Solaris)	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓

Table 2: IBM zSeries and S/390

	z/OS and OS/390	z/VM and VM/ESA	VSE/ESA	Transaction Processing Facility (TPF)	Linux for S/390
ESS Model 800	✓	✓	✓	✓	✓
ESS Models F10 and F20	✓	✓	✓	✓	✓
ESS Models E10 and E20	✓	✓	✓	✓	✓
FICON	✓	✓	✓	✓	✓
ESCON	✓	✓	✓	✓	✓

RQS nº 03/2005 - CI -
CPMI - CORREIOS
Fls. Nº 1364
Doc: 3690

ESS Technical Support Home Page

The ESS Technical Support Home Page contains links to publications, documentation, downloads, utilities, and other resources.

http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/2105

ESS Licensed Internal Code (LIC)

This document contains references to minimum ESS LIC levels. In many cases, the minimum level listed does not represent the latest available LIC level.

Customers are encouraged to keep their ESS at the latest LIC level to take advantage of quality, reliability, and serviceability enhancements and to receive problem determination and fix support.

ESS LIC level 1.5.2 or later, is the currently recommended level.

Host Systems Attachment Guide

The *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* should be referenced to obtain detailed information on attaching servers to the ESS.

Host Adapters

This document contains only limited information regarding host adapter driver levels and other prerequisites. Host adapter firmware, driver, and fix level information is documented in the ESS Fibre Channel Host Bus Adapter (HBA) Support Matrix. This matrix can be found at:

http://ssddom02.storage.ibm.com/hba/hba_support.pdf

Additionally, review host adapter vendor documentation and web pages to obtain information regarding host adapter configuration planning, hardware and software requirements, driver levels, and release notes.

Emulex: http://www.emulex.com/ts/dds.html

JNI: http://www.jni.com/OEM/oem.cfm?ID=4

QLogic: http://www.qlogic.com/support/oem_detail_all.asp?oemid=22

SAN Fabric Products

Fabric product vendor documentation and web pages should be reviewed to obtain information regarding configuration planning, hardware and software requirements, firmware and driver levels, and release notes.

IBM: www.ibm.com/storage/ibmsan/products/sanfabric.html

INRANGE: www.inrange.com/ibm/

McDATA: www.mcdata.com/ibm/

Cisco: www.cisco.com/go/ibm/storage

SAN Volume Controller

The IBM SAN Volume Controller (IBM 2145 Model 4F2) is supported with the ESS Models F10, F20, and 800, and requires ESS LIC level 2.2.0, or later. Refer to the following web page for specific interoperability information on the SAN Volume Controller.

http://www.ibm.com/storage/support/2145

AUSTIN 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1365
Doc: 3690

IBM SAN Data Gateway (SDG)

The SAN Data Gateway (IBM 2108 Model G07) is supported with the ESS Models E10, E20, F10, and F20 for legacy installations only. These installations are encouraged to migrate to native ESS Fibre Channel support.

The ESS Model 800 is not interoperable with the SDG.

Subsystem Device Driver (SDD)

The SDD provides load balancing and enhanced data availability capability in configurations with more than one I/O path between the host server and the ESS. Load balancing can reduce or eliminate I/O bottlenecks that occur when many I/O operations are directed to common devices via the same I/O path. SDD also helps eliminate a potential single point of failure by automatically rerouting I/O operations when a path failure occurs, thereby supporting enhanced data availability capability. The SDD is provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites.

Refer to the *IBM TotalStorage Enterprise Storage Server Subsystem Device Driver User's Guide* for additional information.

Additional SDD information is also available at:

http://www.ibm.com/storage/support/techsup/swtechsup.nsf/support/sddupdates

ESS Application Program Interface (ESS API)

The ESS API can help simplify ESS administration and reduce the total cost of ownership by enabling ESS LUN management activities through implementation of the Storage Management Initiative Specification (SMIS), "Bluefin", as defined by the Storage Networking Industry Association (SNIA). It is implemented through the IBM TotalStorage Common Information Model Agent (CIM Agent) for the ESS, a middleware application that provides a CIM-compliant interface. The ESS API and CIM Agent are provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites. While the CIM Agent is available for only selected operating system environments, it can be used to manage all LUNs within an ESS.

Refer to IBM TotalStorage Common Information Model Agent for the Enterprise Storage Server: Installation and Configuration Guide for additional information.

ESS Command Line Interface (ESS CLI)

The ESS CLI provides an alternate method to perform ESS logical configuration and storage management functions. With the ESS CLI, routine configuration and management tasks can now be automated through their incorporation into scripts and applications, helping to simplify ESS administration and thereby reducing the total cost of ownership. The ESS CLI is provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites. While the ESS CLI is available for only selected operating system environments, it can be used to manage all LUNs within an ESS.

Refer to *IBM TotalStorage Enterprise Storage Server Command Line Interfaces User's Guide* for additional information.

Copy Services Command Line Interface (CS CLI)

The CS CLI enables open systems hosts to invoke and manage FlashCopy and PPRC functions through batch processes and scripts. It provides commands to query the status of ESS volumes and to execute copy services tasks that were previously created using the IBM TotalStorage Enterprise Storage Server Specialist. The CS CLI is provided with the ESS at no additional charge.

Refer to the individual server pages within this document for operating system level requirements and for ESS LIC prerequisites.

Refer to *IBM TotalStorage Enterprise Storage Server Command Line Interfaces User's Guide* for additional information.

Additional CS CLI information is also available at:

http://ssddom02.storage.ibm.com/disk/ess/copyservices.html

ROS nº 02/2005 - CN
CPMI - CORREIOS
Fls. Nº 1366
3690 - 3
Doc:

FlashCopy

FlashCopy provides a point-in-time copy capability for data on the ESS. FlashCopy is designed to create a physical point-in-time copy of the data, with minimal interruption to applications, and makes it possible to access both the source and target copies immediately. FlashCopy is an optional feature on the ESS.

Extended Remote Copy (XRC)

XRC is a combined hardware and software business continuance solution for the zSeries and S/390 environments designed to provide asynchronous mirroring between two ESSs at global distances. XRC is an optional feature on the ESS.

Peer-to-Peer Remote Copy (PPRC)

PPRC is a hardware-based business continuance solution designed to provide real-time mirroring of logical volumes within an ESS or to another ESS. PPRC is an optional feature on the ESS.

IBM supports the use of PPRC in the following modes. Refer to Table 3 for ESS model support and LIC prerequisites.

PPRC Synchronous Mode

PPRC synchronous mode can be used for real-time data mirroring. In this mode, updates made on the primary ESS (local site) are synchronously shadowed to a secondary ESS (remote site).

Since this is a synchronous operation, the distance between the primary and secondary ESS will affect the application response time. Therefore, when operating in this mode, PPRC has a standard maximum supported distance of 103 km between the primary and secondary ESS.

PPRC synchronous mode can be used at distances beyond 103 km with prior approval from IBM. Approval can be requested by submitting a Request for Price Quotation (RPQ). The RPQ should include information on distance between sites, the channel extension technology, the type of telecom line, the amount of network bandwidth, the ESS capacity, and a general description of the workload.

Long Distance Data Copy / Migration

PPRC can be used for long distance data copy or migration of static volumes. Static volumes are volumes that do not have write I/O activity while the PPRC copy of data from the primary to the secondary is in progress.

Since there is no write I/O activity while the PPRC data copy is in progress, the distance between the primary and secondary ESS does not affect application response time. Therefore, when operating in this mode, PPRC can be used with much greater distances between the primary and secondary ESS (as compared to PPRC synchronous mode).

PPRC Extended Distance (PPRC-XD)

PPRC-XD is a non-synchronous long distance copy option suitable for data migration and periodic offsite backup.

With a non-synchronous operation, the distance between the primary and secondary ESS will have only a minimal effect on the application response time. Therefore, PPRC-XD can operate at very long distances.

Asynchronous Cascading PPRC

Asynchronous Cascading PPRC can be used to create three-site or two-site long-distance remote copy solutions. With Asynchronous PPRC, the PPRC secondary volume (involved in a PPRC synchronous relationship) can also simultaneously serve as a PPRC primary volume in a PPRC Extended Distance (PPRC-XD) relationship to the remote site.

RQ91P 05/2005 - CN - CPMI - CORREIOS
Fls. Nº 1367
Doc. 3690

PPRC Channel Extension, DWDM, and Network Connectivity Options

Distances beyond 103 km will require the use of channel extension technology, and the channel extender vendor will determine the maximum distance supported. The vendor should be contacted for their distance capability, line quality requirements, and WAN attachment capabilities.

IBM supports the use of the following products with PPRC:

- ESCON directors
- Channel extenders
  - CNT UltraNet Storage Director
  - INRANGE 9801 Storage Networking System
- DWDMs (Dense Wave Division Multiplexers)
  - Cisco ONS 15540
  - IBM 2029 Fiber Saver
  - Nortel Networks OPTera Metro 5200
  - Nortel Networks OPTera Metro 5300

Refer to Table 3 for ESS LIC prerequisites. Additionally, the product vendors should also be consulted regarding hardware and software prerequisites when using their products in an ESS PPRC configuration. IBM is not responsible for third-party products.

When using PPRC with channel extenders, IBM supports the use of PPRC over all the network technologies that are currently supported by the channel extender products, including Fibre Channel, Ethernet/IP, ATM-OC3, and T1/T3. Evaluation, qualification, approval, and support of PPRC configurations using channel extender products are the sole responsibility of the channel extender vendor. The vendor should be contacted for their distance capability, line quality requirements, and WAN attachment capabilities.

Table 3: Minimum ESS LIC Levels for PPRC

	PPRC Synchronous Mode	PPRC Long Distance Data Copy / Migration	PPRC-XD	Asynchronous Cascading PPRC
ESS Model 800	2.0.0	2.0.0	2.0.0	2.2.0
ESS Models F10 and F20	1.3.0	1.5.0	1.5.2	2.2.0
ESS Models E10 and E20	1.3.0	Not supported	Not supported	Not supported
CNT UltraNet Storage Director	1.5.2	1.5.2	1.5.2	2.2.0
INRANGE 9801 Storage Networking System	1.3.0	1.5.0	1.5.2	2.2.0
IBM 2029 Fiber Saver	1.3.0	1.5.0	1.5.2	2.2.0
Cisco ONS 15540	1.3.4.41	1.5.0	1.5.2	2.2.0
Nortel Networks OPTera Metro 5200	1.3.0	1.5.0	1.5.2	2.2.0
Nortel Networks OPTera Metro 5300	1.3.4.41	1.5.0	1.5.2	2.2.0

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1368
Doc 3690

This page is intentionally left blank.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1369
3690
Doc: Page 8

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
AviiON • 4900 • 5000	DG/UX • 4.2	Adaptec • AHA-2944UW • AHA-4944W	N/A

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1370
3690
Doc:

General notes:

- ESS API – CIM Agent:
  - Not available for DG-UX
- ESS CLI:
  - Not available for DG-UX.
- CS CLI:
  - Not available for DG-UX.
- SDD:
  - Not available for DG-UX.
- Data General servers are not interoperable with the ESS Model 800.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 1371
Doc: 3690 - a

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

HP Server
• rp5400 series
• rp7400
 	
HP 9000 Enterprise Servers
• D-Class
• E-Class
• G-Class
• H-Class
• I-Class
• K-Class
• L-Class
• N-Class
• T-Class
• V-Class
• Enterprise Parallel Servers
	HP-UX
	• 10.20
	• 11.00
	  • PVLINKS
	  • MC/Serviceguard 11.05/09 [1]
	• 11i
	  • PVLINKS
	  • MC/Serviceguard 11.12 and 11.13
		Hewlett-Packard
		• A2969A
		• A4107A
		• A4800A
		• A5159A
		• 28696A
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

HP Server
• rp5400 series
• rp7400
• rp7410 [2]
• rp8400 [2]
• Superdome [2]
 	
HP 9000 Enterprise Servers
• D-Class
• K-Class
• L-Class
• N-Class
• V-Class
	HP-UX
	• 11.00
	  • PVLINKS
	  • MC/Serviceguard 11.05/09 [1]
	• 11i
	  • PVLINKS
	  • MC/Serviceguard 11.12, 11.13, and 11.14
		Hewlett-Packard
		• A3404A
		• A3591B
		• A5158A
		• A6684A
		• A6685A
		• A6795A [3]
			Cisco [3]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2109 Models F16 and F32 [3]
			• 2109 Model M12 [3]
			• 2109 Models S08 and S16
			• 3534 Model F08 [3]
			
			INRANGE
			• FC/9000-64 [4]
			• FC/9000-128 [4]
			• FC/9000- 256 [5]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [3]
			• Sphereon
			  • 3216 [3]
			  • 3232 [3]
			  • 4500 [3]

[1] MC/Serviceguard 11.05/09 can be used with only the K-Class, L-Class, N-Class, and V-Class servers.

[2] Requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.

[3] Requires ESS LIC level 1.5.2, or later.

[4] Requires ESS LIC level 1.3.2.50, or later

[5] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1372
3690
Doc:

General notes:

- Fibre channel:
  - Requires ESS LIC level 1.3.0, or later.
- ESS API – CIM Agent:
  - Not available for HP-UX.
- ESS CLI:
  - Available for HP-UX 11.0, or later.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for all levels of HP-UX.
  - HP-UX 11i requires ESS LIC level 1.5.2, or later.
- SDD:
  - Not available for or interoperable with:
    - HP-UX 10.20.
    - HP-UX 11 32-bit.
    - HP-UX 11i SCSI configurations.
    - MC/Serviceguard
  - HP-UX 11i requires ESS LIC level 1.5.2, or later.
  - Multi-path support is natively available in HP-UX (PVLINKS).
- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Servers:
    - T-Class.
  - Operating systems:
    - HP-UX 10.20.
  - Host adapters:
    - HP A3404A and HP A3591B.
- <u>The following items are not interoperable with ESS Models E10 and E20:</u>
  - ESS CLI.
  - Servers:
    - rp5400, rp7400, rp7410, rp8400, and Superdome.
  - Host adapters:
    - HP A6795A
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1373
Doc. 3690

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
AlphaServer • 800 • 1200 • 2100 • 4000, 4000A • 4100 • 8200, 8400 • DS10, DS20, DS20E • ES40 • GS60, GS60E, GS140	OpenVMS • 6.2-1 H3 • 7.1-2 • 7.2-1, 7.2-2 [7] • 7.3	StorageWorks • KZPBA-CB	N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support
AlphaServer • 800 • 1200 • 4000, 4000A • 4100 • 8200, 8400 • DS10, DS20, DS20E • ES40 • GS60, GS60E, GS140 • GS80, GS160, GS320	OpenVMS • 7.2-2 • 7.3 • 7.3-1 [8]	StorageWorks • KGPSA-CA • KGPSA-DA [8]	IBM • 2109 Model F16 • 2109 Models S08 and S16 • 3435 Model F08

[7] Requires ESS LIC level 1.5.2, or later.

[8] Requires ESS LIC level 2.2.0, or later.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1374
Fls. Nº
3690

General notes:

- Fibre channel:
  - Requires ESS LIC level 2.1.0, or later.
  - Requires ESS Fibre Channel Host Adapter feature #3021, 3023, #3024, or #3025.
  - Not available for the ESS Models E10 and E20.
- Copy services:
  - Requires ESS LIC level 1.5.2, or later.
- ESS API – CIM Agent:
  - Not Available for OpenVMS.
- ESS CLI:
  - Not available for OpenVMS.
- ESS CLI:
  - Available for OpenVMS 7.3, or later.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- SDD:
  - Not available for OpenVMS.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Operating systems:
    - Open VMS 6.2.

- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - Fibre channel.
  - Copy services.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1375
Doc: 3690

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

AlphaServer
• 800
• 1200
• 2100
• 4000, 4000A
• 4100
• 8200, 8400
• DS10, DS20, DS20E
• ES40
• GS60, GS60E, GS140
	Tru64 UNIX
	• 4.0D, 4.0E
	• 4.0F, 4.0G
	  • ASE 1.6
	• 5.0A
	  • TruCluster 5.0A
	• 5.1
	  • TruCluster 5.1
	• 5.1A [1]
	  • TruCluster 5.1A
		StorageWorks
		• KZPBA-CB
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

AlphaServer
• 800
• 1200
• 2100
• 4000, 4000A
• 4100
• 8200, 8400
• DS10, DS20, DS20E
• ES40
• GS60, GS60E, GS140
• GS80, GS160, GS320 [1]
	Tru64 UNIX
	• 4.0F, 4.0G
	  • ASE 1.6
	• 5.0A
	  • TruCluster 5.0A
	• 5.1
	  • TruCluster 5.1
	• 5.1A [1]
	  • TruCluster 5.1A
	• 5.1B [2]
	  • TruCluster 5.1B
		StorageWorks
		• KGPSA-BC
		• KGPSA-CA
		• KGPSA-DA [2]
			IBM
			• 2109 Model F16 [1]
			• 2109 Models S08 and S16
			• 3534 Model F08 [1]

[1] Requires ESS LIC level 1.5.2, or later.

[2] Requires ESS LIC level 2.2.0, or later.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1376
Fls. Nº
Doc: 3690

HEWLETT-PACKARD SERVERS – TRU64 UNIX

General notes:

- Fibre channel:
  - Requires ESS LIC level 1.3.3.27, or later.
- Copy services:
  - Requires ESS LIC level 1.5.2, or later.
  - Not available for the ESS Models E10 and E20.
- ESS API – CIM Agent:
  - Not Available for Tru64 UNIX.
- ESS CLI:
  - Not available for Tru64 UNIX.
- CS CLI:
  - Available for Tru64UNIX 4.0F, 4.0G, 5.1, 5.1A, and 5.1B.
  - Requires ESS LIC level 1.5.2, or later.
  - Not available for the ESS Models E10 and E20.
- SDD:
  - Not available for Tru64 UNIX.
  - Multi-path support is natively available in Tru64 UNIX.
- Boot device support:
  - The ESS can be used as a boot device on servers running Tru64 UNIX 5.0A and 5.1. This function requires ESS LIC level 1.3.3, or later. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Operating systems:
    - Tru64 UNIX 4.0 (all levels).

<u>The following items are not interoperable with the ESS Models E10 and E20:</u>

- Copy services.
- CS CLI.
- Servers:
  - AlphaServers GS80, GS160, and GS320.
- Operating systems:
  - Tru64 UNIX 5.1A and 5.1B.
- Fabric products:
  - IBM 3534 Model F08.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1377
Fls. Nº
3690
Doc.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

9406 Advanced Series
• 300, 310, 320
• 500, 510, 530
 	
9406
• 620, 640, 650
• 720, 730, 740
• S20, S30, S40
 	
iSeries
• 820, 830, 840
• SB2, SB3
	OS/400
	• Version 3
	  • V3R1 @
	  • V3R2 @
	  • V3R6 @
	  • V3R7 @
	• Version 4
	  • V4R1 @
	  • V4R2 @
	  • V4R3 @
	  • V4R4 @
	  • V4R5
	• Version 5
	  • V5R1
	  • V5R2 [1]
		IBM iSeries and AS/400
		• FC 6501
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

iSeries
• 270
• 820, 830, 840, 890[1]
• 800, 810, 825, and 870 [3]
	OS/400
	• Version 5
	  • V5R1
	  • V5R2 [1]
	
	Linux [2]
	• SuSE Linux Enterprise Server 7 for iSeries
	
	UnitedLinux 1.0 [4]
	• SuSE Linux Enterprise Server 8 (SP 1)
		IBM iSeries
		• FC 0612
		• FC 2766
			IBM
			• 2109 Model F16 [1]
			• 2109 Models S08 and S16
			• 3534 Model 1RU
			• 3534 Model F08 [1]

[1] Requires ESS LIC level 1.5.2, or later.

[2] Requires Linux kernel level 2.4.13, and OS/400 V5R2, or later.

[3] Requires ESS LIC level 1.5.2, or later and OS/400 V5R2, or later.

[4] Requires Linux kernel level 2.4.19, OS/400 V5R2, or later, and ESS LIC level 2.1.1, or later.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1378
3690
Doc:

General notes:

- Fibre channel support:
  - Requires ESS LIC Level 1.3.2, or later.
- Copy services:
  - PPRC-XD requires OS/400 Version 5 Release 1, or later.
- ESS API – CIM Agent:
  - Not Available for OS/400.
- ESS CLI:
  - Not available for OS/400.
- CS CLI:
  - Not available for OS/400.
- SDD:
  - Not available for OS/400.

- <u>The following items are not interoperable with the Model 800:</u>
  - Operating systems:
    - OS/400 Version 3 (all release levels).
    - OS/400 Version 4 (all release levels except V4R5).
  - Fabric products:
    - IBM 3534 Model 1RU.

- <u>The following items are not interoperable with the Models F10 and F20:</u>
  - Operating systems:
    - SuSE Linux Enterprise Server 7 for iSeries.

- <u>The following items are not interoperable with the Models E10 and E20:</u>
  - Servers
    - iSeries 800, 810, 825, 870, and 890.
  - Operating systems:
    - OS/400 Version 5 Release 2.
    - OS/400 Version 4 (all release levels except Release 5).
    - SuSE Linux Enterprise Server 7 for iSeries.
    - UnitedLinux 1.0.
  - Fabric products:
    - IBM 2109 Models F16, S08, and S16.
    - IBM 3534 Model F08.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1379
3690
Doc:

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support
2000 • E100 • E200 • E320 • E400, E410 • xSeries 430	ptx (DYNIX) [1] • 4.4.7, 4.4.8, 4.4.9, 4.4.10 • 4.5.1, 4.5.2, 4.5.3 • 4.6.1	IBM NUMA-Q • IOC-0210-54	IBM • 2109 Models S08 and S16

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1380
3690
Doc:

[1] ptx general notes:
- ptx 4.4.7, 4.4.8, 4.4.9, and 4.4.10 interoperability is available only via RPQ (NSBO).
- ptx 4.4.10 requires ESS LIC level 1.4.0, or later.
- ptx 4.5.1 requires service pack 3.

General Notes:

- NUMA-Q support requires ESS LIC level 1.2.1, or later.
- ESS API – CIM Agent:
  - Not available for ptx.
- ESS CLI:
  - Not available for ptx.
- CS CLI:
  - Available for all levels of ptx.
- SDD:
  - Not available for ptx.

The following items are not interoperable with the ESS Model 800:

- Operating systems:
  - ptx 4.4.7, 4.4.8, 4.4.9, and 4.4.10.
  - ptx 4.5.1 and 4.5.2.
  - ptx 4.6.1.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1381
Doc: 3690

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
pSeries • 610 Models 6C1, 6E1 • 615 Models 6C3 and 6E3 • 620 Models 6F0, 6F1 • 630 Models 6C4, 6E4 [1] • 640 Model B80 • 650 Model 6M2 [1] • 655 Model 651 [1] • 660 Models 6H0, 6H1, 6M1 • 670 Model 671 [1] • 680 Model S85 • 690 Model 681 [1] 7012 • 397 • G40 7013 • 590, 591, 595, 59H • J30, J40, J50 • S70, S7A 7015 • 99J, 99K • R20, R24, R30, R40, R50 • S70, S7A 7017 • S70, S7A, S80 7024 • E20, E30 7025 • F30, F40, F50, F80 • H70 '026 • H10, H50, H70, H80 • M80 7043 • 270 7044 • 170 • 270	AIX • Version 4 • 4.2.1 @ • 4.3.1 @ • 4.3.2 @ • 4.3.3 • Version 5 • 5.1 • 5.2 [7] HACMP [2] • 4.2.2 • 4.3.1 • 4.4.0, 4.4.1 • 4.5.0 [3]	IBM pSeries and RS/6000 • FC 2412 • FC 6204 • FC 6207	N/A

[1] ESS LIC level prerequisites for servers:
- The pSeries 630, 650, and 655 require ESS LIC level 1.5.2, or later.
- The pSeries 670 requires ESS LIC level 1.5.1, or later.
- The pSeries 690 requires ESS LIC level 1.4.0, or later.

[2] Refer to Table 4 for additional HACMP support information.

[3] Requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F20 and F20.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1382
Doc. 3690

Fibre Channel

Servers

pSeries
- 610 Models 6C1, 6E1
- 615 Models 6C3 and 6E3
- 620 Models 6F0, 6F1
- 630 Models 6C4, 6E4 [1]
- 640 Model B80
- 650 Model 6M2 [1]
- 655 Model 651 [1]
- 660 Models 6H0, 6H1, 6M1
- 670 Model 671 [1]
- 680 Model S85
- [illegible] Model 681 [1]

[illegible]13
- S70, S7A

7015
- S70, S7A

7017
- S70, S7A, S80

7025
- F50, F80
- H70

7026
- H50, H70, H80
- M80

7043
- 270

7[illegible]
- 170
- 270

Operating Systems

AIX
- Version 4
  - 4.3.3
- Version 5
  - 5.1
  - 5.2 [7]

HACMP [2]
- 4.3.1
- 4.4.0, 4.4.1
- 4.5.0 [3]

UnitedLinux 1.0 [9]
- SuSE Linux Enterprise Server 8 (SP 1)

Host Adapters

IBM pSeries and RS/6000
- FC 6227
- FC 6228
- FC 6239 [10]

Fabric Support

Cisco [5]
- MDS 9216
- MDS 9509

IBM
- 2103 Model H07 [4]
- 2109 Models F16 and F32 [5]
- 2109 Model M12 [5]
- 2109 Models S08 and S16
- 3534 Model F08 [5]

INRANGE
- FC/9000-64 [6]
- FC/9000-128 [6]
- FC/9000- 256 [8]

McDATA
- ED-5000
- ES-3016 and ES-3032
- Intrepid
  - 6064
  - 6140 [5]
- Sphereon
  - 3216 [5]
  - 3232 [5]
  - 4500 [5]

[4] The IBM 2103 is supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[5] Requires ESS LIC level 1.5.2, or later.

[6] Requires ESS LIC level 1.3.2.50, or later.

[7] Requires ESS LIC level 2.0.1, or later, for the ESS Model 800 and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[8] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[9] Requires Linux kernel level ppc64-2.4.19-186, and ESS LIC level 2.1.1, or later. UnitedLinux 1.0 is supported with only host adapter FC 6228 and only with IBM or McDATA fabric products.

[10] Requires ESS LIC level 2.1.1, or later.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. - Nº 1983
Doc: 3690 - 15

General Notes:

- Fibre channel:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for AIX 5.1.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for AIX 4.3.3, 5.1, and 5.2.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.

CS CLI:

- Available for AIX 4.3.2, 4.3.3, 5.1, and 5.2.

- SDD:
  - Available for AIX 4.3.1, or later.
- Boot device support:
  - The ESS is supported as a boot device on pSeries, RS/6000, and RS/6000 SP servers that support Fibre Channel boot capability. This support requires ESS LIC level 1.4.0, or later, and native Fibre Channel attachment to the ESS. Boot device support when using SDD requires ESS LIC level 2.1.0, or later. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.
- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Servers:
    - Micro Channel Architecture (MCA) servers, including 7012-397, 7013-59x, 7013-Jxx, 7015-99x, and 7015 Rxx.
  - Operating systems:
    - AIX 4.2.1, 4.3.1 and 4.3.2.
    - HACMP 4.2.2 and 4.3.1.
  - Host adapters:
    - IBM FC 2412.
  - Fabric products:
    - IBM 2103 Model H07.
- <u>The following items are not interoperable with the ESS Models E10 and E20</u>
  - ESS API.
  - ESS CLI.
  - SDD
    - Boot Device Support.
  - Operating systems:
    - AIX 5.2.
    - HACMP 4.5.0.
    - UnitedLinux 1.0.
  - Servers:
    - 615 Models 6C3 and 6E3.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232 and 4500.

CPMI CORREIOS
1384
Fls. Nº
3690
Doc:

Table 4: AIX and HACMP Support Matrix

	ESS Model 800	ESS Models F10 and F20	ESS Models E10 and E20	SDD
AIX 4.2.1 with HACMP 4.2.2	--	--	SCSI	--
AIX 4.3.3 with HACMP 4.2.2	--	--	SCSI	--
AIX 4.3.3 with HACMP 4.3.1	--	SCSI Fibre Channel	SCSI Fibre Channel	Yes
AIX 4.3.3 with HACMP 4.4.0	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes
AIX 4.3.3 with HACMP 4.4.1	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes [1]
AIX 5.1 with HACMP 4.4.0	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes
AIX 5.1 with HACMP 4.4.1	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	Yes [1]
AIX 5.1 with HACMP 4.5.0	SCSI Fibre Channel	SCSI Fibre Channel	--	Yes
AIX 5.2 with HACMP 4.5.0	SCSI Fibre Channel	SCSI Fibre Channel	--	Yes

[1] RS/6000 SP with SDD and HACMP 4.4.1 requires AIX 5.1 ML2 with ESS LIC level 1.4.0, or later.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1385
3690
Doc:

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

9076 Models 2xx, 3xx, 4xx, 50x, 55x, and T70 with the following nodes:
 	
Micro Channel
• FC 2002: 62MHz Thin Node
• FC 2003: 66MHz Thin Node
• FC 2004: 66MHz Thin Node 2
• FC 2005: 77MHz Wide Node
• FC 2006: 604 High Node
• FC 2007: 35MHz Wide Node
• FC 2008: 120MHz Thin Node
• FC 2009: 604E High Node
• FC 2022: 160MHz Thin Node
 	
PCI
• FC 2050: 332 MHz SMP Single Thin
• FC 2051: 332 MHz SMP Wide Node
• FC 2052: POWER3 SMP Thin Node
• FC 2053: POWER3 SMP Wide Node
• FC 2054: POWER3 SMP High Node
• FC 2055: SP Expansion I/O Unit
• FC 2056: POWER3 375MHz SMP Thin
• FC 2057: POWER3 375MHz SMP Wide
• FC 2058: POWER3 375MHz SMP High
	AIX
	• Version 4
	  • 4.2.1 @
	  • 4.3.1 @
	  • 4.3.2 @
	  • 4.3.3
	• Version 5
	  • 5.1 ML2 [1]
	
	PSSP [2]
	• 3.1, 3.1.1
	• 3.2
		IBM RS/6000
		• FC 2412
		• FC 6204
		• FC 6207
		• FC 6209
			N/A

...03/2005 - CN - CPMI - CORREIOS
Fls Nº 1386
3690
Doc:

[1] Requires ESS LIC level 1.4.0, or later.

[2] Refer to Table 5 for additional PSSP information. Refer to Table 4 (pSeries and RS/6000 server section) for HACMP information.

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

9076 Models 2xx, 3xx, 4xx, 50x, 55x, and T70 with the following PCI nodes:
• FC 2050: 332 MHz SMP Single Thin Node
• FC 2051: 332 MHz SMP Wide Node
• FC 2052: POWER3 SMP Thin Node
• FC 2053: POWER3 SMP Wide Node
• FC 2054: POWER3 SMP High Node
• FC 2055: SP Expansion I/O Unit
• FC 2056: POWER3 375MHz SMP Thin Node
• FC 2057: POWER3 375MHz SMP Wide Node
• FC 2058: POWER3 375MHz SMP High Node
	AIX
	• Version 4
	  • 4.3.3
	• Version 4
	  • 5.1 ML2 [1]
	
	PSSP [2]
	• 3.1.1
	• 3.2
	• 3.4
		IBM RS/6000
		• FC 6227
		• FC 6228
			Cisco [4]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [3]
			• 2109 Models F16 and F32 [4]
			• 2109 Model M12 [4]
			• 2109 Models S08 and S16
			• 3534 Model F08 [4]
			
			INRANGE
			• FC/9000-64 [5]
			• FC/9000-128 [5]
			• FC/9000- 256 [6]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [4]
			• Sphereon
			  • 3216 [4]
			  • 3232 [4]
			  • 4500 [4]

[3] The IBM 2103 is supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1.5.2, or later.

[5] Requires ESS LIC level 1.3.2.50, or later.

[6] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

RQS nº 03/2005 - CN -
CPML - CORREIOS
Fls. Nº 1387
3690
Doc:

General Notes:

- Fibre channel:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for AIX 5.1 ML2.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for AIX 4.3.3 and 5.1.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.

  CS CLI:
  - Available for AIX 4.3.2, 4.3.3, and 5.1.
- SDD:
  - Available for AIX 4.3.3, or later
  - Requires ESS LIC level 1.3.2.50, or later.
  - Refer to Table 5 for additional information.
- Boot device support:
  - The ESS is supported as a boot device on pSeries, RS/6000, and RS/6000 SP servers that support Fibre Channel boot capability. This support requires ESS LIC level 1.4.0, or later, and native Fibre Channel attachment to the ESS. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.
- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Servers:
    - Micro Channel Architecture (MCA) servers, including 7012-397, 7013-59x, 7013-Jx, 7015-99x, and 7015 Rxx.
  - Operating systems:
    - AIX 4.2.1, 4.3.1 and 4.3.2.
    - HACMP 4.2.2 and 4.3.1.
  - Host adapters:
    - IBM FC 2412.
  - Fabric products:
    - IBM 2103 Model H07.
- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - ESS API.
  - ESS CLI.
  - Operating systems:
    - HACMP 4.5.0
  - Fabric products:
    - Cisco MDS 9216, and 9509.
    - IBM 2109 Model F32.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 4500

RQS nº 03/2005 - CN
CPMI - CORREIOS
1388
Fls. Nº
Doc: 3690 - 1

Table 5: AIX, PSSP, and SDD Support Matrix

	ESS Model 800	ESS Models F10 and F20	ESS Models E10 and E20	SDD Level
AIX 4.3.2 with: • PSSP and RVSD 3.1.0 • GPFS 1.2	--	SCSI	SCSI	--
AIX 4.3.3 with: • PSSP and RVSD 3.1.1 • GPFS 1.2	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	1.2.1.3
AIX 4.3.3 with: • PSSP and RVSD 3.2 • GPFS 1.3 or 1.4	SCSI Fibre Channel	SCSI Fibre Channel	SCSI Fibre Channel	1.2.1.3
AIX 5.1 with: • PSSP 3.4 • GPFS 1.5	Fibre Channel	Fibre Channel	Fibre Channel	1.3.1.1

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1389
Fls. Nº
3690
Doc:

ESCON

Servers	Operating Systems	Host Adapters	Fabric Support
zSeries z800 • IBM 2066 zSeries z900 and z990 • IBM 2064 S/390 Parallel Enterprise Server • IBM 9672 Generation 3 • IBM 9672 Generation 4 • IBM 9672 Generation 5 • IBM 9672 Generation 6 ES/9000 • IBM 9021 • IBM 9121 • IBM 9221 ES/3090 • IBM 3090 S/390 Multiprise 3000 Enterprise Server • IBM 7060 S/390 Multiprise 2000 Enterprise Server • IBM 2003	z/OS • Version 1 Release 1 • Version 1 Release 2 • Version 1 Release 3 • Version1 Release 4 [1] z/OS.e • Version 1 Release 3 • Version 1 Release 4 [1] OS/390 • Version 1 Release 3 @ • Version 2 Release 4 @ • Version 2 Release 5 @ • Version 2 Release 6 @ • Version 2 Release 7 @ • Version 2 Release 8 @ • Version 2 Release 9 @ • Version 2 Release 10 z/VM • Version 3 Release 1 @ • Version 4 Release 1 @ • Version 4 Release 2 • Version 4 Release 3 • Version 4 Release 4 [5] VM/ESA • Version 2 Release 2 @ • Version 2 Release 3 @ • Version 2 Release 4 @ VSE/ESA • Version 2 Release 1 @ • Version 2 Release 2 @ • Version 2 Release 3 @ • Version 2 Release 4 @ • Version 2 Release 5 • Version 2 Release 6 • Version 2 Release 7 Transcription Processing Facility (TPF) [2] • Version 4 Release 1 Linux for S/390 • SuSE Linux Enterprise Server for S/390 • Turbolinux Server 6 for zSeries and S/390 • SuSE SLES 8 for zSeries and S/390 [3]	All ESCON host adapter features offered on the servers are supported.	IBM • 9032 Model 002 • 9032 Model 003 • 9032 Model 005

[1] Requires ESS LIC level 1.5.2, or later.

[2] In the TPF environment, PPRC and FlashCopy require ESS LIC level 1.5.0, or later.

[3] Requires ESS LIC Level 2 1.1 or later, direct connect only.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1390
3690
Doc:

FICON

Servers

zSeries z800
- IBM 2066

zSeries z900 and z990
- IBM 2064

S/390 Parallel Enterprise Server
- IBM 9672 Generation 5
- IBM 9672 Generation 6

Operating Systems

z/OS
- Version 1 Release 1
- Version 1 Release 2
- Version 1 Release 3
- Version 1 Release 4 [1]

z/OS.e
- Version 1 Release 3
- Version 1 Release 4 [1]

OS/390
- Version 2 Release 8 @
- Version 2 Release 9 @
- Version 2 Release 10

z/VM
- Version 3 Release 1 @
- Version 4 Release 1 @
- Version 4 Release 2
- Version 4 Release 3
- Version 4 Release 4 [5]

VM/ESA
- Version 2 Release 3 @
- Version 2 Release 4 @

VSE/ESA
- Version 2 Release 3 @
- Version 2 Release 4 @
- Version 2 Release 5
- Version 2 Release 6
- Version 2 Release 7

Transaction Processing Facility (TPF) [2]
- Version 4 Release 1

Linux for zSeries and S/390 [3]
- SuSE SLES 8

Host Adapters

zSeries
- FC 2315
- FC 2318
- FC 2319
- FC 2320

S/390
- FC 2314
- FC 2316

Fabric Support

INRANGE
- FC/9000-64
- FC/9000-128
- FC/9000-256 [4]

McDATA
- ED-5000
- Intrepid 6064
- Intrepid 6140 [1]

RQS nº 03/2005 - CN - CPMI - CORREIOS
1391
Fls. Nº
3690
Doc:

[4] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[5] Requires ESS LIC level 2.2.0, or later.

Fibre Channel Protocol (FCP)

Servers	Operating Systems	Host Adapters	Fabric Support
zSeries z800 • IBM 2066 zSeries z900 and z990 • IBM 2064	UnitedLinux 1.0 • SuSE SLES 8 (SP 2)	zSeries • FC 2315 • FC 2318 • FC 2319 • FC 2320	IBM • 2109 Model F16 • 2109 Models S08 and S16 INRANGE • FC/9000-64 • FC/9000-128 McDATA • Intrepid 6064

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1392
Doc: 3690

General Notes:

- ESCON:
  - IBM eServer Integrated Platform for e-business on zSeries, and S/390 G5 and G6:
    - Supported on ESS Models F20 and F10, and requires ESS LIC level 2.1.1, or later.
    - Requires zVM Version 4 Release 3.
    - Requires Linux SLES 7, with kernel level 2.4.7.
- FICON:
  - Requires ESS LIC level 1.4.0, or later.
  - FICON is not supported on the ESS Models E10 and E20.
- Fibre Channel Protocol (FCP):
  - Requires ESS LIC level 2.1.1, or later.
  - FCP is not supported on the ESS Models E10 and E20.
  - Multipath support is available with LVM.
- Copy Services
  - Supported in the Linux for zSeries and S/390 environment with SuSE SLES 8.
- ESS API – CIM Agent:
  - Not available for zSeries and S/390 operating systems.
- ESS CLI:
  - Not available for zSeries and S/390 operating systems.
- CS CLI:
  - Not available for zSeries and S/390 operating systems.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Operating systems:
    - OS/390 levels 1.3, 2.4, 2.5, 2.6, 2.7, 2.8, and 2.9.
    - VM/ESA levels 2.2 and 2.3.
    - VSE/ESA levels 2.1, 2.2, and 2.3.
    - IBM eServer Integrated Platform for e-business on zSeries.

- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - FCP.
  - FICON.
  - Operating systems:
    - z/OS level 1.4.
    - z/OS.e level 1.4.
    - z/VM level 4.4.
    - VSE/ESA level 2.7.
    - IBM eServer Integrated Platform for e-business on zSeries.
  - Fabric products:
    - McDATA Intrepid 6140.
  - ESS copy services in the TPF environment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1393
3690
Doc:

This page is intentionally left blank.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1394
Doc: 3690 -

Fibre Channel

Servers

Pentium Pro or later processors
- 200 MHz processor or faster
- 128 MB memory or greater
- Excludes IBM Netfinity 3000 and IBM PC Server 325

IBM eServer BladeCenter [8]
- BladeCenter HS20

Operating Systems

Red Hat Linux
- 7.1 [1]
- 7.2 [1]
- 7.3 [1]

Red Hat Enterprise Linux Advanced Server
- 2.1 [2]

SuSE Linux
- 7.2
- 7.3

SuSE Linux Enterprise Server (SLES)
- 7 [3]

UnitedLinux 1.0 [7]
- SuSE Linux Enterprise Server 8 (SP 1 and SP 2a)

Host Adapters

Emulex
- LP9002L / LP9002DC [4]
- LP9402DC [4]
- LP9802 [4]

IBM BladeCenter
- P/N 48P7062

QLogic
- QLA2300F
- QLA2310F / QLA2310FL [4]
- QLA2340/L / QLA2342/L [5]

Fabric Support

Cisco [4]
- MDS 9216
- MDS 9509

IBM
- 2109 Models F16 and F32 [4]
- 2109 Model M12 [4]
- 2109 Models S08 and S16
- 3534 Model F08 [4]

INRANGE
- FC/9000-64
- FC/9000-128
- FC/9000- 256 [6]

McDATA
- ED-5000
- ES-3016 and ES-3032
- Intrepid
  - 6064
  - 6140 [4]
- Sphereon
  - 3216 [4]
  - 3232 [4]
  - 4500 [4]

---

[1] Red Hat 7.x requires kernel level 2.4.18-24.7xbigmen, and ESS LIC level 2.1.1, or later.

[2] Red Hat Enterprise Advanced Server 2.1 requires kernel level 2.4.9-e.16 (enterprise or summit for x440 server), or kernel level 2.4.9-e.24 QU2 (enterprise), and ESS LIC 2.1.1, or later.

[3] SuSE Linux Enterprise Server 7 Update requires kernel level k_smp-2.4.18-224, and ESS LIC level 2.1.1, or later.

[4] Requires ESS LIC level 1.5.2, or later.

[5] Requires ESS LIC level 2.1.0, or later.

[6] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[7] Requires SP 1 kernel level k_smp-2.4.19-233, SP 2a kernel level k_smp-2.4.19-304, and ESS LIC level 2.2.0, or later.

[8] Requires ESS LIC level 2.1.1, or later, and Red Hat Linux Advanced Server 2.1, kernel level 2.4.9.e.16. The following fabric products are supported. IBM 2109 Model F16, IBM 3534 Model F08, INRANGE, and McDATA (excluding ED-5000).

RQS nº 03/2005 - CN
CPMI - CORREIOS
1395
Fls. Nº
3690

General Notes:

- Linux is interoperable with only the ESS Models F10, F20, and 800.
- ESS API – CIM Agent:
  - Available for Red Hat Linux 7.2.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for Red Hat 7.2, and 7.3.
  - Available for UnitedLinux 1.0 (SLES 8).
  - Requires ESS LIC level 2.1.0, or later.
- CS CLI:
  - Available for all levels of Linux.
- SDD:
  - Available for Red Hat 7.2 and Red Hat Enterprise Advanced Server 2.1.
  - Available for SuSE 7.3 and SuSE Linux Enterprise Server 7.
  - Available for UnitedLinux 1.0 (SLES 8).
  - SDD is not interoperable with BladeCenter.
- The following SuSE and Redhat levels are no longer recommended with the ESS. If problems are encountered with existing installations, you may be required to update your Linux configuration to a higher level before problem determination can take place.
  - Red Hat Linux 7.1 running kernel level 2.4.9.
  - Red Hat Linux 7.2 running kernel level 2.4.9-31.
  - Red Hat Linux Advanced Server 2.1 running kernel levels 2.4.9-e.8 and 2.4.9-e.10 (enterprise).
  - SuSE Linux 7.2 running kernel level 2.4.9.
  - SuSE Linux 7.3 running kernel level k_smp-2.4.16-22.
  - SuSE Linux Enterprise Server (SLES) 7 running kernel level 2.4.18-134.

  <u>The following items are not interoperable with the Model 800:</u>
  - Operating systems:
    - Red Hat Linux 7.1.
    - SuSE Linux 7.2.
- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - BladeCenter.
  - ESS API
  - Host Adapters:
    - Emulex LP9402DC and LP9802.
  - Fabric products
    - Cisco MDS 9216 and MDS 9509
    - INRANGE FC/9000- 256
  - Operating Systems:
    - UnitedLinux 1.0.

RQS nº 03/2005 - CN - CPMI – CORREIOS
Fls. Nº 1396
Doc: 3690

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later processors
• 200 MHz processor or faster
• 128 MB memory or greater
	Novell NetWare
	• 4.11 @
	• 4.2
	  • Standby Server
	• 5.0
	  • Cluster Services 1.00
	  • Cluster Services 1.01
	• 5.1
	  • Cluster Services 1.01
	• 6.0 [1]
		Adaptec
		• AHA-2944UW
		
		IBM xSeries / Netfinity
		• P/N 08L6517 [2]
		• P/N 59H3900
		
		QLogic
		• QLA1041
			N/A

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later processors
• 200 MHz processor or faster
• 128 MB memory or greater
• Excludes IBM Netfinity 3000 and IBM PC Server 325
	Novell NetWare
	• 4.2
	  • Standby Server
	• 5.0
	  • Cluster Services 1.00
	  • Cluster Services 1.01
	• 5.1
	  • Cluster Services 1.01
	• 6.0 [1]
	  • Cluster Services 1.6
		Emulex
		• LP9002L / LP9002DC [1]
		• LP9402DC [1]
		• LP9802 [1]
		
		IBM xSeries / Netfinity
		• P/N 01K7297
		• P/N 00N6881
		• P/N 19K1246
		• P/N 24P0960
		
		QLogic
		• QLA2100F
		• QLA2200F
		• QLA2310F / QLA2310FL [1]
		• QLA2340/L / QLA2342/L [1]
			Cisco [1]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [3]
			• 2109 Models F16 and F32 [1]
			• 2109 Model M12 [1]
			• 2109 Models S08 and S16
			• 3534 Model 1RU [3]
			• 3534 Model F08 [1]
			
			INRANGE
			• FC/9000-64 [4]
			• FC/9000-128 [4]
			• FC/9000- 256 [5]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064 [4]
			  • 6140 [4]
			• Sphereon
			  • 3216 [4]
			  • 3232 [4]
			  • 4500 [1]

[1] Requires ESS LIC level 1.5.2, or later.
- Planned availability is 4Q03 for the Emulex LP9402DC and LP9802 host adapter interoperability.

[2] Host adapter IBM P/N 08L6517 includes an incorrect SCSI cable for ESS attachment. Order ESS feature number 9701 / 2801 (10 meter) or feature number 9702 / 2802 (20 meter) to obtain the correct SCSI cable to use this host adapter with the ESS.

[3] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1 5.2, or later, and NetWare 5.1 or later.

[5] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1397
3690
Doc:

General Notes:

- Fibre Channel support:
  - Requires ESS LIC level 1.3.0, or later.
- Clustering support:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Not available for NetWare.
- ESS CLI:
  - Not available for NetWare.
- CS CLI:
  - Available for NetWare 4.2 and NetWare 5.1, or later.
  - NetWare 6.0 requires ESS LIC 2.1.0, or later.

SDD:

- Refer to the *IBM TotalStorage Enterprise Storage Server Subsystem Device Driver User's Guide* for support information when running NetWare 5.1 and 6.0 with SDD.
- Requires NetWare 5.1, or later, and ESS LIC level 2.1.0, or later.
- Not interoperable with the Emulex LP9002L / LP9002DC, LP9402DC, and LP9802.
- Not available for the ESS Model E10 and E20.
- NetWare 6.0 cluster services supported on fibre channel only.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Operating systems:
    - NetWare 4.11 and 4.2.
  - Host adapters:
    - IBM P/N 01K7297.
    - QLogic QLA1041 and QLA2100F.
  - Fabric products:
    - IBM 2103 Model H07.
    - IBM 3534 Model 1RU.

- <u>The following items are not interoperable with the ESS Models E10 and E20:</u>
  - CS CLI:
    - NetWare 6.0.
  - SDD.
  - Operating systems:
    - NetWare 6.0.
  - Host adapters:
    - Emulex LP90002L.
    - Emulex LP9002L / LP9002DC.
    - Emulex LP9402DC and LP9802.
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
  - Fabric products:
    - IBM 2109 Models F32, and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support
Pentium Pro or later 32 bit processors • 200 MHz processor or faster • 128 MB memory or greater	Microsoft Windows NT • Server 4.0 • Server 4.0, Enterprise Edition including Microsoft Cluster Server (MSCS) Microsoft Windows 2000 • Server • Advanced Server including Cluster service Microsoft Windows Server 2003 [6] • Standard Edition • Enterprise Edition including cluster service	Adaptec • AHA-2944UW IBM Netfinity/xSeries • P/N 08L6517 [1] • P/N 59H3900 QLogic • QLA1041 Symbios • LSI8751D	N/A

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1399
Doc: 3690

[1] Host adapter IBM 08L6517 includes an incorrect SCSI cable for ESS attachment. Order ESS feature number 9701 / 2801 (10 meter) or feature number 9702 / 2802 (20 meter) to obtain the correct SCSI cable to use this host adapter with the ESS.

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Pentium Pro or later 32 bit processors
• 200 MHz processor or faster
• 128 MB memory or greater
• Excludes IBM Netfinity 3000 and IBM PC Server 325
 	
IBM eServer BladeCenter [7]
• BladeCenter HS20
	Microsoft Windows NT
	• Server 4.0
	• Server 4.0, Enterprise Edition including Microsoft Cluster Server (MSCS)
	
	Microsoft Windows 2000
	• Server
	• Advanced Server including Cluster service
	• Datacenter Server
	
	Microsoft Windows Server 2003 [6]
	• Standard Edition
	• Enterprise Edition including cluster service
	• Datacenter Edition including cluster server
		Emulex
		• LP7000E
		• LP8000
		• LP9002L / LP9002DC [2]
		• LP9402DC [2]
		• LP9802 [2]
		
		IBM BladeCenter
		• P/N 48P7062
		
		IBM Netfinity/xSeries
		• P/N 01K7297
		• P/N 00N6881
		• P/N 19K1246
		• P/N 24P0960
		
		QLogic
		• QLA2100F
		• QLA2200F
		• QLA2310F / QLA2310FL [2]
		• QLA2340/L / QLA2342/L [2]
			Cisco [2]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [3]
			• 2109 Models F16 and F32 [2]
			• 2109 Model M12 [2]
			• 2109 Models S08 and S16
			• 3534 Model F08 [2]
			• 3534 Model 1RU [3]
			
			INRANGE
			• FC/9000-64 [4]
			• FC/9000-128 [4]
			• FC/9000- 256 [5]
			
			McDATA
			• ED-5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064 [2]
			  • 6140 [2]
			• Sphereon
			  • 3216 [2]
			  • 3232 [2]
			  • 4500 [2]

[2] Requires ESS LIC level 1.5.2, or later.

[3] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[4] Requires ESS LIC level 1.3.2.50, or later.

[5] Requires ESS LIC level 2 1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[6] Requires ESS LIC level 2.2.0, or later Windows 2003 is not supported on the Emulex LP7000E, QLogic QLA2100F, and IBM P/N 01K7297 host adapters, and the Cisco fabric switches.

[7] Requires ESS LIC level 2.1.1, or later, and is supported on only Windows 2000 (non-clustered configurations). The following fabric products are supported: IBM 2109 Model F16, IBM 3534 Model F08, INRANGE, and McDATA (excluding ED-5000).

RQS nº 03/2005 - CN - CPMI - CORREIOS
1400
Fls. Nº
Doc 3690

General Notes:

- Fibre channel support:
  - Requires ESS LIC level 1.2.0, or later.
- ESS API – CIM Agent:
  - Available for all levels of Windows 2000.
  - Requires ESS LIC level 2.1.1, or later.
  - Not available for the ESS Models E10 and E20.
- ESS CLI:
  - Available for all levels of Windows 2000, and Windows Server 2003.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for all levels of Windows NT, Windows 2000, and Windows Server 2003.
- SDD:
  - Available for all levels of Windows NT and Windows 2000 and Windows 2003 (see additional notes on following page).
  - Load balancing is not available in Windows NT or Windows 2000 cluster configurations.
- Boot device support:
  - The ESS is supported as a boot device on Windows 2000 servers that support Fibre Channel boot capability. This support requires ESS LIC level 2.2.0, or later, with host adapters QLA2310F / QLA2310FL, and QLA2340 / QLA2342L. Requires SDD level 1.4.0.0. Refer to the *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide* for additional information.

- <u>The following items are not interoperable with the ESS Model 800:</u>
  - Host adapters:
    - Emulex LP7000E.
    - IBM 01K7297.
    - QLogic QLA1041 and QLA2100F.
    - Symbios SYM8751D.
  - Fabric products:
    - IBM 2103 Model H07.
    - IBM 3534 Model 1RU.

- <u>The following items are not interoperable with the ESS Models E10 and E20</u>
  - BladeCenter.
  - ESS CLI.
  - Operating systems:
    - Datacenter Server.
  - Host adapters:
    - Emulex LP9002L / LP9002DC.
    - Emulex LP9802 and LP9402DC.
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
  - ESS API.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32 and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1401
Doc: 5690 - a

General Notes (cont.):

- **Windows NT**
  - Enterprise Edition with Microsoft Cluster Server (MSCS) support requires ESS LIC level 1.3.0, or later.
- **Windows 2000**
  - Server and Advanced Server:
    - Requires ESS LIC Level 1.2.0, or later.
    - Advanced Server with Cluster service support requires ESS LIC level 1.3.0, or later.
    - When using SDD, Advanced Server with Cluster service support requires ESS LIC level 1.4.0, or later. The QLogic QLA2100F is not supported in this configuration.
  - Datacenter Server:
    - Requires ESS LIC level 1.5.0, or later.
    - When using SDD, Datacenter Server requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.
    - For a list of specific ESS configurations supported with Datacenter Server, refer to the Microsoft Hardware Compatibility Listing (HCL) at http://www.microsoft.com/hcl/. Enter "Enterprise Storage Server" and "All Product Categories" as the search criterion. Use the IBM RPQ process to request support for additional ESS configurations.
- **Windows 2003**
  - When using clustering with SDD, Windows 2003 is not supported on Emulex LP8000, LP9002L / LP9002DC, LP9402DC, LP9802 host adapters.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1402
Doc: 3690

Fibre Channel

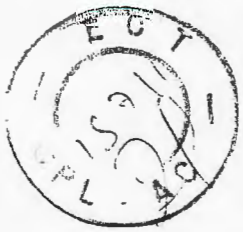
Servers	Operating Systems	Host Adapters	Fabric Support
Origin Servers • 200 • 2100 • 2200 • 2400 • 2800	IRIX • 6.5.13 • 6.5.14 • 6.5.15 • 6.5.16 • 6.5.17	SGI • PCI-FC-1P-OPT • PCI-FC-1P-OPT-A • PCI-FC-1POPT-B [3] • PCX-FC-2POPT-B [3]	IBM[1] • 2109 Models S08 and S16 • 2109 Model F16 • 3534 Model F08

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 1403
3690
Doc:

[1] Cascaded switches are not supported

[3] Requires ESS LIC level 2.2.0, or later.

General Notes:



- SGI support requires ESS LIC level 2.1.1, or later.
- ESS API – CIM Agent:
  - Not available for IRIX.
- ESS CLI:
  - Not available for IRIX.
- CS CLI:
  - Not available for IRIX.
- SDD:
  - Not available for IRIX.

The following items are not interoperable with the ESS Models E10 and E20:

- SGI Servers
  - Origin 200, 2100, 2200, 2400, and 2800

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1404
Doc. 3690 -

SCSI

Servers	Operating Systems	Host Adapters	Fabric Support

Enterprise
• 220R, 250, 420R, 450
• 3000, 4000, 5000, 6000
• 3500, 4500, 5500, 6500
• 10000
 	
Netra
• 1125
 	
SPARCcenter / SPARCserver
• 1000, 1000E
• 2000, 2000E
 	
Ul
1, 2, 5, 10, 20, 30, 60, 80
	Solaris
	• 2.5.1
	• 2.6
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2 and 1.3
	• 7
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2 and 1.3
	• 8
	  • VERITAS Volume Manager with DMP
	  • 3.1.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.3
		Sun
		• X1062A
		• X1065A
		• X6541A
			N/A

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1405
Fls. Nº
3690
Doc:

Fibre Channel

Servers	Operating Systems	Host Adapters	Fabric Support

Enterprise
• 220R, 250, 420R, 450
• 3000, 4000, 5000, 6000
• 3500, 4500, 5500, 6500
• 10000
 	
Netra
• 1125
 	
SPARCcenter / SPARCserver
• 1000, 1000E
• 2000, 2000E
 	
n Fire
• V120 [1]
• V280R [1]
• V480 [1]
• V880 [1]
• 3800 [1]
• 4800 [1], 4810 [1], 6800 [1]
• 12K [2], 15K [2]
 	
Ultra
• 1,2, 5, 10, 20, 30, 60, 80
	Solaris
	• 2.6
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2, 1.3, 2.0, and 3.5 [3]
	• 7
	  • VERITAS Volume Manager with DMP
	  • 3.1 and 3.2
	  • VERITAS Cluster Server
	  • 1.1.2, 1.3 2.0, and 3.5 [3]
	• 8
	  • Sun Cluster 3.0 with MPxIO 4.1, or later [10]
	  • VERITAS Volume Manager with DMP
	  • 3.1.1, 3.2, and 3.5
	  • VERITAS Cluster Server
	  • 1.3, 2.0, and 3.5 [3]
	• 9 [3,7]
	  • VERITAS Volume Manager with DMP
	  • 3.5
	  • VERITAS Cluster Server
	  • 3.5
		JNI
		• FC64-1063-N
		• FCC-6562 / FCC2-6562 [3]
		• FCX-6562 / FCX2-6562 [3]
		• FCI-1063-N
		• FCE-1473-N [1]
		• FCE-6460-N [1]
		
		Emulex
		• LP8000
		• LP8000S [4]
		• LP9002C [3]
		• LP9002L / LP9002DC [1]
		• LP9002S [1]
		• LP9402DC [1]
		• LP9802 [1]
		
		QLogic
		• QLA2200F
		• QLA2310F / QLA2310FL [1]
		• QLA2340/L / QLA2342/L [1]
		• QCP2340 [9]
		
		Sun [10]
		• 6727A
		• 6767A
		• 6768A
		• 6799A
			Cisco [1]
			• MDS 9216
			• MDS 9509
			
			IBM
			• 2103 Model H07 [5]
			• 2109 Models F16 and F32 [1]
			• 2109 Model M12 [1]
			• 2109 Models S08 and S16
			• 3534 Model F08 [1]
			
			INRANGE
			• FC/9000-64 [6]
			• FC/9000-128 [6]
			• FC/9000- 256 [8]
			
			McDATA
			• ED 5000
			• ES-3016 and ES-3032
			• Intrepid
			  • 6064
			  • 6140 [1]
			• Sphereon
			  • 3216 [1]
			  • 3232 [1]
			  • 4500 [1]

[1] Requires ESS LIC level 1.5.2, or later.

[2] Requires ESS LIC level 2.0.0, or later, for the ESS Model 800 and ESS LIC level 2.1.0, or later, for the ESS Models F10 and F20.

[3] Requires ESS LIC level 2.1.0, or later.

[4] Requires ESS LIC level 1.5.0, or later.

[5] Supported for distance solutions only. Multiple initiators or targets on the same loop are not supported.

[6] Requires ESS LIC level 1.3.2.50, or later.

[7] Requires Veritas Filesystem VXFS V 3.5 REV=GA06

[8] Requires ESS LIC level 2.1.0, or later, for the ESS Model 800, and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[9] Requires 2.1.1, or later.

[10] Requires ESS LIC level 2.2.0, or later. Sun Clustering 3.0 with MPxIO is supported only with the Sun host adapters.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1406
3690
Doc:

General Notes:

- Fibre channel support:
  - Requires ESS LIC level 1.3.0, or later.
- ESS API – CIM Agent:
  - Not Available for Solaris.
- ESS CLI:
  - Available for Solaris 8.
  - Requires ESS LIC level 2.1.0, or later.
  - Not available for the ESS Models E10 and E20.
- CS CLI:
  - Available for only Solaris 2.6, 7, 8, and 9.
- SDD:
  - Available for only Solaris 2.6, 7, and 8. (SDD is not supported in Sun Cluster environments.)
  - Solaris 7, or later is required when using the Emulex LP8000.
  - In clustered configurations, VERITAS Cluster Manager and VERITAS Volume Manager with DMP should be used instead of SDD.
  - SDD is not supported in Sun Cluster environments.
- VERITAS:
  - Support for VERITAS Volume Manager is limited to Solaris 7 when using ESS LIC level 1.0.x, 1.1.x or 1.2.x.

- The following items are not interoperable with the ESS Model 800:
  - Operating systems:
    - Solaris 2.5.1.
  - Fabric products:
    - IBM 2103 Model H07.
- The following items are not interoperable with the ESS Models E10 and E20

  ESS CLI.

  Servers:
  - Sunfire V120, V280R, V480, V880, 3800, 4800, 4810, 6800, 12K, and 15K.
  - Host adapters:
    - JNI FCC2-6562, FCS-6562 / FCX2-6562, FCE-1473-N and FCE6460-N.
    - Emulex LP9002C, LP9002L / LP9002DC, LP9002S, and LP9402DC, and LP9802.
    - QLogic QLA2310F / QLA2310FL and QLA2340 / QLA2342L.
    - Sun 6727A, 6767A, 6768A, and 6799A.
  - Operating Systems:
    - Sun cluster 3.0 and MPxIO.
  - Fabric products:
    - Cisco MDS 9216 and MDS 9509.
    - IBM 2109 Models F32, and M12.
    - IBM 3534 Model F08.
    - INRANGE FC/9000- 256
    - McDATA Intrepid 6140.
    - McDATA Sphereon 3216, 3232, and 4500.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1407
3690
Doc:

NETWORK ATTACHED STORAGE (NAS)

NAS Servers[1]	Fabric Support
NAS Gateway 300 • 5196 Model G00 • 5196 Model G01 • 5196 Model G02 [3] • 5196 Model G25 • 5196 Model G26 • 5196 Model G27 [2]	IBM • 2109 Models S08 and S16 • 2109 Models F16, and F32 [3] INRANGE • FC/9000 McDATA • ED-5000

[1] NAS interoperability requires ESS LIC level 1.3.2.49, or later.

[2] Requires ESS LIC level 2.0.1, or later, for the ESS Model 800 and ESS LIC level 1.5.2, or later, for the ESS Models F10 and F20.

[3] Requires ESS LIC level 1.5.2 or later.

RQS nº 03 2005 - CN -
CPMI - CORREIOS
Nº 1408
3690
Doc: Page 47

General Notes:

- The following items are not interoperable with the ESS Models E10 and E20
  - NAS Gateway 300
    - 5196 Model G00
    - 5196 Model G01
    - 5196 Model G02
    - 5196 Model G25
    - 5196 Model G26
    - 5196 Model G27

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1409
Doc: 3690

APPENDIX A: ESS HOST ADAPTERS AND CABLES

Table 6: ESS Host Adapter Features

Feature Number	Features Description	Supported ESS Models	Minimum ESS LIC Level
3002	SCSI Host Adapter	Exx / Fxx / 800	1.0.0
3011	Standard ESCON Host Adapter	Exx / Fxx	1.0.0
3012	Enhanced ESCON Host Adapter	Fxx / 800	1.4.0
3013	64-bit ESCON Host Adapter	800	2.1.0
3019 [1]	Fibre Channel Host Adapter (interim NUMA-Q)	Exx / Fxx	1.1.0
3020 [1]	Fibre Channel Host Adapter (interim)	Exx / Fxx	1.1.0
3021	Fibre Channel / FICON Host Adapter (long wave)	Fxx	1.4.0
3022	Fibre Channel Host Adapter (short wave)	Exx / Fxx	1.2.0
3023	Fibre Channel / FICON Host Adapter (short wave)	Fxx	1.4.0
3024	2Gb Fibre Channel / FICON Host Adapter (long wave)	800	2.0.0
3025	2Gb Fibre Channel / FICON Host Adapter (short wave)	800	2.0.0

Table 7: ESS Fibre Channel / FICON Cable Features

Specify Feature	Optional Feature	Feature Description	Cable Length
9750	2850	9 micron Fibre Cable (SC connectors)	31 meters
9751	2851	9 micron Fibre Cable (SC / LC connectors)	31 meters
9752	2852	9 micron Fibre Cable (LC connectors)	31 meters
9753	2853	9 micron Fibre Cable (SC / LC connectors)	2 meters (pigtail)
9760	2860	50 micron Fibre Cable (SC connectors)	31 meters
9761	2861	50 micron Fibre Cable (SC / LC connectors)	31 meters
9762	2862	50 micron Fibre Cable (LC connectors)	31 meters
9763	2863	50 micron Fibre Cable (SC / LC connectors)	2 meters (pigtail)

Table 8: ESS SCSI Cable Features

Specify Feature	Optional Feature	Feature Description	Cable Length
9701	2801	Ultra SCSI	10 meters
9702	2802	Ultra SCSI	20 meters
9703	2803	SCSI-2 Fast/Wide	10 meters
9704	2804	SCSI-2 Fast/Wide	20 meters
9705	2805	SCSI-2 Fast/Wide (AS/400)	10 meters
9706	2806	SCSI-2 Fast/Wide (AS/400)	20 meters
9707	2807	SCSI-2 Fast/Wide (Sun PCI/HP PCI dual port)	10 meters
9708	2808	SCSI-2 Fast/Wide (Sun PCI/HP PCI dual port)	20 meters
9709	2809	SCSI-2 Fast/Wide (HP single port)	10 meters
9710	2810	SCSI-2 Fast/Wide (HP single port)	20 meters

[1] Withdrawn from marketing.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1410
Doc: 3690

APPENDIX B: HOST ADAPTER PRODUCTS

Table 9: SCSI Host Adapters

Adapter	Description	ESS Cable Feature
Adaptec AHA-2944UW	PCI-to-Ultra Wide Differential SCSI Host Adapter	9701 or 9702
Adaptec AHA-4944W	Quad Channel PCI-to-Fast and Wide Differential SCSI Host Adapter	9701 or 9702
Hewlett-Packard A4800A	Fast/Wide Ultra Differential SCSI-2 (PCI)	9709 or 9710
Hewlett-Packard A4107A	Fast/Wide Differential SCSI-2 (HP-HSC)	9703 or 9704
Hewlett-Packard A2969A	20 MB Fast/Wide Differential SCSI-2 (HP-HSC)	9703 or 9704
Hewlett-Packard A5159A	Dual Port Fast/Wide Differential SCSI-2 (PCI)	9707 or 9708
Hewlett-Packard 28696A	Fast/Wide Differential SCSI-2 (HP-PB)	9703 or 9704
IBM AS/400 FC 6501	Tape/Disk Device Controller	9705 or 9706
IBM Netfinity P/N 59H3900	3449 Adapter Card	9701 or 9702
IBM Netfinity P/N 08L6517	Adapter card + cable + terminator	9701 or 9702
IBM RS/6000 FC 2412	Enhanced SCSI-2 Differential Fast/Wide Adapter/A	9703 or 9704
IBM RS/6000 FC 6204	PCI Universal Differential Ultra SCSI Adapter	9701 or 9702
IBM RS/6000 FC 6207	PCI Differential Ultra SCSI Adapter	9701 or 9702
IBM RS/6000 FC 6209	PCI SCSI-2 Fast/Wide Differential Adapter	9703 or 9704
QLogic QLA1041	PCI-to-Ultra SCSI Host Adapter	9701 or 9702
Storage Works KZPBA-CB	Ultra SCSI Differential Adapter (PCI)	9701 or 9702
Sun X1062A	SCSI-2 Fast/Wide Differential (SBus)	9701 or 9702
Sun X1065A	Ultra SCSI (SBus)	9701 or 9702
Sun X6541A	Ultra SCSI-2, Fast/Wide Differential Dual Channel (PCI)	9707 or 9708
Symbios SYM8751D	PCI-to-Fast/Ultra Wide Differential SCSI Host Adapter	9701 or 9702

SDS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1411
Doc. 3690

Table 10: Fibre Channel Host Adapters

Adapter	Description
Emulex LP7000E	LightPulse Fibre Channel PCI Host Adapter (32 bit)
Emulex LP8000	LightPulse Fibre Channel PCI Host Adapter (1Gb)
Emulex LP8000S	LightPulse Fibre Channel SBus Host Adapter (1Gb)
Emulex LP9000C	LightPulse Fibre Channel cPCI Host Bus Adapters (2Gb)
Emulex LP9002L	LightPulse Fibre Channel PCI Host Adapter (2Gb)
Emulex LP9002DC	Light Pulse Fibre Channel PCI Host Adapter (2Gb) (two ports)
Emulex LP9002S	LightPulse Fibre Channel SBus Host Adapter (2Gb)
Emulex LP9402DC	LightPulse Fibre Channel PCI-X Host Adapter (2Gb) (two ports)
Emulex LP9802	LightPulse Fibre Channel PCI-X Host Adapter (2GB)
Hewlett-Packard A3404A	1063 Mbps Fibre Channel K Class Adapter (HP-HSC)
Hewlett-Packard A3591B	1062 Mbps Fibre Channel Adapter (HP-HSC)
Hewlett-Packard A5158A	PCI Tachlite Fibre Channel Adapter
Hewlett-Packard A6684A	HSC Tachlite Fibre Channel Adapter
Hewlett-Packard A6685A	HSC Tachlite Fibre Channel Adapter
Hewlett-Packard A6795A	PCI Tachlite 2Gb Fibre Channel Adapter
IBM iSeries FC0612	Linux Direct Attachment
IBM iSeries FC 2766	PCI Fibre Channel Disk Controller
IBM Netfinity P/N 01K7297	Netfinity PCI Fibre Channel Adapter
IBM Netfinity P/N 00N6881	Netfinity FAStT Host Adapter
IBM NUMA-Q IOC-0210-54	Fibre Channel PCI Adapter
IBM pSeries FC 6227	Fibre Channel Adapter for PCI Bus
IBM pSeries FC 6228	Fibre Channel Adapter 64-Bit for PCI Bus (2Gb)
IBM pSeries FC 6239	Fibre Channel Adapter 64-bit for PCI Bus (2Gb)
IBM xSeries P/N 48P7061	BladeCenter HS20 Fibre Channel Expansion Card
IBM xSeries P/N 48P7062	BladeCenter 2-port Fibre Channel Switch Module
JNI FC64-1063-N	FibreStar 64-Bit SBus Fibre Channel Host Bus Adapter
JNI FCC-6562	FibreStar CompactPCI-to-Fibre Channel Host Bus Adapter (2Gb)
JNI FCC2-6562	FibreStar CompactPCI-to-Fibre Channel Host Bus Adapter (2Gb) (two ports)
JNI FCX-6562	FibreStar PCI-X-to-Fibre Channel Host Bus Adapter (2Gb)
JNI FCX2-6562	FibreStar PCI-X-to-Fibre Channel Host Bus Adapter (2Gb) (two ports)
JNI FCI-1063-N	FibreStar 32-Bit PCI-to-Fibre Channel Host Bus Adapter
JNI FCE-1473-N	FibreStar 2Gb 64-bit SBus-to-Fibre Channel Host Bus Adapter
JNI FCE-6460-N	FibreStar 2Gb 64-bit PCI-to-Fibre Channel Host Bus Adapter
QLogic QCP2340	64-Bit 66MHz PCI 2Gb Fibre Channel Adapter
QLogic QLA2100F	64-Bit PCI-to-Fibre Channel Adapter
QLogic QLA2200F	64-Bit PCI-to-Fibre Channel Adapter (33MHz or 66 MHz)
QLogic QLA2300F	65-Bit PCI-to-Fibre Channel Adapter (66MHz)
QLogic QLA2310F	66MHz PCI-X Fibre Channel Adapter
QLogic QLA2310FL	66MHz PCI-X Fibre Channel Adapter (low profile)
QLogic QLA2340/L	133MHz PCI-X Fibre Channel Adapter (low profile)
QLogic QLA2342/L	133MHz PCI-X Fibre Channel Adapter (two ports; low profile)
SGI PCI-FC-1P-OPT	Optical SW 1GB Fibre Channel Adapter

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1412
Doc: 3690

Table 10: Fibre Channel Host Adapters (cont.)

Adapter	Description
SGI PCI-FC-1P-OPT-A	Optical SW 1GB Fibre Channel Adapter
SGI PCI-FC-1POPT-B	Optical SW 2 GB Fibre Channel Adapter
SGI PCX-FC-2POPT-B	Optical SW 2GB Fibre Channel Adapter (two ports)
StorageWorks KGPSA-BC	64-bit / 33 MHz PCI-to-Fibre Channel Host Bus Adapter
StorageWorks KGPSA-CA	64-bit / 33 MHz PCI-to-Fibre Channel Host Bus Adapter
StorageWorks KGPSA-DA	64-bit / 66MHz PCI 2Gb Fibre Channel Adapter
Sun 6727A	64-Bit PCI-to-Fibre Channel Adapter (33MHz or 66 MHz) (dual port)
Sun 6767A	66MHz PCI-X 2Gb Fibre Channel Adapter
Sun 6768A	133MHz PCI-X 2Gb Fibre Channel Adapter (two ports; low profile)
Sun 6799A	64-Bit PCI-to-Fibre Channel Adapter (33MHz or 66 MHz)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1413
Doc 3690

APPENDIX C: SAN FABRIC PRODUCTS

Fibre Channel / FICON Intermix

The ESS supports Fibre Channel / FICON intermix on the INRANGE FC/9000 Fibre Channel Director (IBM 2042 Models 001 and 128) and the McDATA ED-6064 (open-open mode) Enterprise Fibre Channel Director (IBM 2032 Model 064). With intermix, both FCP (Fibre Channel Protocol) and FICON upper level protocols can be supported within the same director when deployed independently by port. Cascading of directors is not currently supported with Fibre Channel / FICON intermix.

Fibre Channel / FICON intermix support requires ESS LIC level 1.5.2, or later. Implementation details and operational information for using intermix are available at the INRANGE and McDATA websites.

Table11: SAN Fabric Products

Product	IBM Machine Type and Model or Part Number	Description
Cisco MDS 9216	IBM 2062 Model D01	Cisco Multilayer Fabric Switch (2Gb, 48-port)
Cisco MDS 9509	IBM 2062 Models D07 / T07	Cisco Multilayer Director (2Gb, 224-port)
IBM 2103 Model H07		IBM Fibre Channel Storage Hub
IBM 2109 Model F16	P/N 2109F16	IBM TotalStorage SAN Switch (2Gb, 16-port)
IBM 2109 Model F32	P/N 2109F32	IBM TotalStorage SAN Switch (2Gb, 32-port)
IBM 2109 Model M12		IBM TotalStorage SAN Switch (2Gb, 64-port)
IBM 2109 Model S08	P/N 2109S08	IBM TotalStorage SAN Switch (1Gb, 8-port)
IBM 2109 Model S16	P/N 2109S16	IBM TotalStorage SAN Switch (1Gb, 16-port)
IBM 3534 Model F08	P/N 3534F08	IBM TotalStorage SAN Switch (2Gb, 8-port)
IBM 3534 Model 1RU	P/N 35341RU	IBM TotalStorage SAN Managed Hub
INRANGE FC/9000-64	IBM 2042 Model 001	INRANGE FC/9000 Fibre Channel Director (2Gb, 64-port)
INRANGE FC/9000-128	IBM 2042 Model 128	INRANGE FC/9000 Fibre Channel Director (2Gb, 128-port)
INRANGE FC/9000-256	IBM 2042 Model 256	INRANGE FC/9000 Fibre Channel Director (2Gb, 256-port)
McDATA ES-3016	IBM 2031 Model 016	McDATA ES-3016 Fabric Switch (1Gb, 16-port)
McDATA ES-3032	IBM 2031 Model 032	McDATA ES-3016 Fabric Switch (1Gb, 32-port)
McDATA Sphereon 3216	IBM 2031 Model 216	McDATA Sphereon Fabric Switch (2Gb, 16-port)
McDATA Sphereon 3232	IBM 2031 Model 232	McDATA Sphereon Fabric Switch (2Gb, 32-port)
McDATA Sphereon 4500	IBM 2031 Model 224	McDATA Sphereon Fabric Switch (2Gb, 24-port)
McDATA ED-5000	IBM 2032 Model 001	McDATA ED-5000 Fibre Channel Director
McDATA Intrepid 6064	IBM 2032 Model 064	McDATA Intrepid 6064 Director (2Gb, 64-port)
McDATA Intrepid 6140	IBM 2032 Model 140	McDATA Intrepid 6140 Director (2Gb, 140-port)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº
1414
Doc: 3690

APPENDIX D: REVISION HISTORY

May 13, 2003

Unless stated otherwise, these items require ESS LIC level 2.2.0, or later, which has a planned availability of June 27, 2003.

ESS Copy Services
- Peer-to-Peer Remote Copy (PPRC) Version 2
- FlashCopy Version 2

Servers
- iSeries 800, 810, 825, and 870
- Sun Fire V120, V280R, and V480
- zSeries 990

Channel Extenders/DWDMs
- Nortel Networks OPTera Metro 5200

Operating Systems, Path Management, and Clustering
- Hewlett Packard OpenVMS 7.3-1
- Hewlett Packard Serviceguard 11.14
- Hewlett Packard Tru64 5.1B
- Sun Cluster 3.0 including MPxIO
- Sun VERITAS Cluster Server 3.5

Operating Systems, Path Management, and Clustering (cont.)
- UnitedLinux 1.0 (Intel): SLES 8 (including CLI and SDD support)
- Windows Server 2003 (including CLI support)
- Windows 2000 Boot Support (including SDD support)
- zSeries VSE/ESA Version 2 Release 7
- zSeries z/VM Version 4 Release 4

Host Adapters
- Emulex LP9802 and LP9402DC (Intel (NetWare, Windows) Sun)
- QLogic QCP2340 (Sun)
- SGI PCI-FC-1POPT-B
- Storage Works KGPSA-DA (HP OpenVMS and Tru64)
- Sun 6727A, 6767A, 6768A, and 6799A.

February 17, 2003

Unless stated otherwise, these items require ESS LIC level 2.1.1, or later, which has a planned availability of February 21, 2003 for the Models 800, F10 and F20.

General
- ESS API: CIM Agent support (AIX, Intel (Linux, Windows 2000)
- SGI Origin Servers

Operating Systems, Path Management, and Clustering
- AIX 5.2 with HACMP 4.5
- Veritas Cluster server for Sun Solaris 9
- Linux (Intel): New kernel levels

Other

End of Service and Support for various Linux/Redhat (Intel) Levels. Refer to the Linux (Intel) server page for specific information.

SAN Fabric
- INRANGE FC/9000-256 (HP, RS/6000, RS/6000 SP, Intel (Linux, Netware, Windows), and Sun)

ECT 1570 2

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1415
Doc. 3690

November 22, 2002

Unless stated otherwise, these items require ESS LIC level 2.1.0, or later, which has a planned availability of November 22, 2002 for the Model 800 and January 31, 2003 for the Models F10 and F20.

General

- Planned availability for ESS Models F10 and F20 interoperability changed to January 31, 2003 for the following items. Additionally ESS LIC level has changed to ESS LIC level 2.1.0 or later.
  - HP rp7410, rp8400, and Superdome
  - HACMP 4.5.0
  - Red Hat Linux 7.2 (Intel)
  - Windows 2000 Datacenter (Intel)
  - SuSE Linux 7.3 (Intel)
  - Sun Fire 12K, and 15K

Servers

- IBM pSeries 650 Model 6M2 and pSeries 655 Model 651
- Sun Fire V880, and 3800

Operating Systems, Path Management, and Clustering

- SuSE Linux Enterprise Server 7 (iSeries)
- AIX 5.2
- Solaris 9

SAN Fabric

- IBM 2109 Model F32 (HP, RS/6000, Intel (Linux, NetWare, Windows), Sun, and NAS)
- McData Sphereon 4500 (HP, RS/6000, Intel (Linux, Netware, Windows), and Sun)
- IBM 2109 Model F16 (NAS)

NAS Fabric

- NAS Gateway 300, Model G27

Adapters

- Emulex LP9002DC (Intel (Linux, Netware, Windows), and Sun)
- JNI FCC-6562 (Sun)

October 22, 2002

Unless stated otherwise, these items require ESS LIC level 2.1.0, or later, which has a planned availability of November 22, 2002 for the Model 800 and January 31, 2003 for the Models F10 and F20

General

- OpenVMS: Fibre Channel support

Configuration Management

- ESS CLI (AIX, HP-UX, Linux (Intel), Solaris, and Windows 2000)

Copy Services CLI

- NetWare 6.0
- OpenVMS

Operating Systems, Path Management, and Clustering

- Linux (Intel): Red Hat Advanced Server 2.1 (including copy services CLI and SDD)
- Linux (Intel): SuSE Linux Enterprise Server 7 (including copy services CLI and SDD)
- NetWare: SDD support

Host Adapters

- Emulex LP9002C (Sun)
- JNI FCC2-6562 and FCX-6562 / FCX2-6562 (Sun)
- QLA2340 / QLA2342L (Linux (Intel), NetWare, and Sun)

Other

Removed footnotes for host adapter restrictions; information has been moved to the Host Bus Adapter Support Matrix.

October 7, 2002

Servers

- IBM iSeries 890

Operating Systems, Path Management, and Clustering

- HACMP 4 5.0
- HP MC/Serviceguard 11.13
- HP-UX 11 (32-bit support for SCSI)

Operating Systems, Path Management, and Clustering (con't)

- OpenVMS 7.2-2
- z/OS and z/OS.e Version1 Release 4

SAN Fabric

- McDATA Intrepid 6140 (HP, IBM pSeries, Intel (Linux, NetWare, Windows), and Sun

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1416
Doc. 3650

Manual 05

IBM TotalStorage TM
UltraScalable Tape Library 3584

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1417
Fls. Nº
3690
Doc:

An UltraScalable, ultra-flexible tape library for backup and archival solutions

IBM TotalStorage™ UltraScalable Tape Library 3584

IBM TotalStorage UltraScalable Tape Library 3584 with 16 frames

Highlights

- ***Offers 16-frame capacity, performance, and reliability for midrange and network tape storage environments***
- ***Provides an UltraScalable solution to help protect your technology investment***
- ***Patented Multi-path Architecture helps increase configuration flexibility with logical library partitioning***
- ***Adheres to widely supported Linear Tape-Open™ (LTO) Ultrium™ design specifications***
- ***Offers native switched fabric 2Gb Fibre Channel LTO Ultrium 2 Drives***

IBM TotalStorage UltraScalable Tape Library—A flexible solution

From midrange systems to large-scale server-based operations, the IBM TotalStorage UltraScalable Tape Library is designed to handle backup, archive, and disaster recovery data storage needs with ease.

Advanced features

The IBM TotalStorage UltraScalable Tape Library 3584 now supports up to 16 frames housing a maximum of 6,881 tape cartridges and 192 Ultrium tape drives. Support for the IBM TotalStorage Ultrium 2 Tape Drive more than doubles tape drive performance over the first generation LTO Ultrium Tape Drive and is designed to support up to 35MB/sec native data transfer rates (70MB/sec with 2:1 compression). In addition, with the use of the new IBM TotalStorage LTO Ultrium 200GB Data Cartridge, the IBM TotalStorage Ultrium 2 Tape Drive doubles the tape cartridge capacity up to 200GB native capacity (400GB with 2:1 compression).

The IBM TotalStorage Ultrium 2 Tape Drives can read and write original LTO Ultrium data cartridges at first generation Ultrium 1 capacities with improved performance. The Ultrium 2 tape drives and cartridges can be resident in the same 3584 Library frame with first generation Ultrium tape drives and Cartridges. The UltraScalable Tape Library is designed with a variety of advanced features. IBM's Multi-path Architecture is designed to simultaneously attach heterogeneous servers and applications to LTO logical library partitions, including mixed Ultrium drives and media.

Remote management capabilities using a Web browser provides library control and configuration. Simple Network Management Protocol (SNMP) functionality is also included. Hot swap drives, data path failover and load balancing and redundant power supplies offer enhanced availability. New control path failover for AIX, dual AC power and 110 volt power options are also available.

Software support

You can maximize the power of the UltraScalable Tape Library by managing it with industry-leading tape management solutions such as Tivoli®

ROS nº 03/2005 - CN - CPMI - CORREIOS
1418
Fls: Nº
3690
Doc:

IBM TotalStorage UltraScalable Tape Library 3584 at a glance

Model number	L32—LTO base frame; D32—LTO expansion frame

Characteristics

Tape drive type	IBM LTO Ultrium 2 or 1
Number of frames	One base frame and up to 15 expansion frames
Number of drives	Up to 192: L32—1 to 12 LTO; D32—0 to 12 LTO
Number of tape cartridges	Up to 6,881: L32—87 to 281; D32—396 to 440
Number of logical libraries	Up to 192: L32—up to 12; D32—up to 12
Capacity[1,2]	2,752 TB compressed, in a 16-frame configuration with four drives L32 (1-4 drives)—Up to 112.4 TB/frame compressed; 56.2 TB native D32 (0 drives)—Up to 176 TB/frame compressed; 88.0 TB native
Sustained data transfer rate[2]	LTO Ultrium 2: Up to 70 MB/sec compressed; 35 MB/sec native
Measured aggregate sustained data rate[2]	Up to 47.4TB/hour with 192 LTO Ultrium 2 tape drives (compressed)[2]
Media type	IBM TotalStorage LTO Ultrium 200 GB Data Cartridge (P/N 08L9870) IBM TotalStorage LTO Cleaning Cartridge (P/N 35L2086)
Dimensions (L32 or D32)	70.9" H x 28.5" W x 59.8" D (1800 mm x 725 mm x 1520 mm)
Max. weight	L32—1236.0 lb (539.4 kg); D32—1161.9 lb (527.0 kg)
Warranty	One year; IBM On-site Repair (IOR)

Operating environment

Temperature	16° to 32° C (60.8° to 89.6° F)
Relative humidity	20% to 80% (non-condensing)
Wet bulb maximum	23.0° C (73.4° F)
Electrical power	8 amps at 200-240 VAC; 1.6 kVA, 1.4 kilowatt nominal 12 amps at 100-127 VAC; 1.2kVA, 1.2 Kilowatt nominal
Noise level	7.5 bels; 51 dBA operating

Attachment and systems support[3]

The IBM 3584 features LTO Fibre Channel, LVD Ultra2/Wide or Ultra160 SCSI and HVD Ultra SCSI interfaces, attaching to IBM @server pSeries™, IBM @server iSeries™, IBM @server xSeries™, RS/6000®, RS/6000 SP, AS/400®, and Netfinity® systems, and non-IBM servers and workstations

Operating systems support[3]

Device driver support is available for AIX®; OS/400®; Windows NT®; Windows® 2000; Windows 2003; Sun Solaris; and HP-UX.

[1] Capacity depends on the number of drives installed versus the number of tape cartridges used
[2] Based on 2:1 compression
[3] For latest information, consult Technical Support at www.ibm.com/totalstorage/lto

Storage Manager or other storage software.

Why IBM LTO?

IBM LTO Ultrium drives share best-of-breed technology. Advanced multi-track recording capabilities, state-of-the-art magneto-resistive (MR) heads, and a sophisticated track following servo system work together to produce extremely high recording densities. New Ultrium 2 drive enhancements include digital speed matching, power management, channel calibration and 512 data tracks. Error correction code (ECC) function and Statistical Analysis and Reporting System (SARS) help support data integrity.

For more information

For more information, contact your IBM representative or your IBM Business Partner. For updated attachment, supported operating system, media product, and storage management software information, visit www.ibm.com/totalstorage/lto.

© International Business Machines Corporation 2003

IBM Systems Group
Removable Media Storage Solutions
9000 S. Rita Road
Tucson, AZ 85744
United States

Produced in the United States
06-03
All Rights Reserved

IBM, AIX, AS/400, @server, iSeries, Netfinity, OS/400, pSeries, RS/6000, and xSeries, are registered trademarks of International Business Machines Corporation.

Linear Tape-Open, LTO, the LTO logo, Ultrium, and the Ultrium logo are U.S. trademarks of HP, IBM, and Seagate. Tivoli is a registered trademark of Tivoli Systems, Inc. DLT tape is a registered trademark of Quantum. Windows and Windows NT are registered trademarks of Microsoft Corporation. Other company, product, and service names may be trademarks or registered trademarks of their respective companies.

Other company, product, and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

IBM hardware products are manufactured from new parts, or new and used parts. In some cases, the hardware product may not be new and may have been previously installed. Regardless, IBM warranty terms apply.

Product data is accurate as of initial publication and is subject to change without notice.

Photography depicts design models. Actual product may show slight variations.

G225-6853-05

CEMI - 1419
Fls. Nº 3690

Manual 06

The IBM LTO Ultrium Tape Libraries Guide
(REDBOOK)

FLS Nº 03/2005 - CN - CPMI - CORREIOS
1420
Fls Nº
3690
Doc.

The IBM LTO Ultrium Tape Libraries Guide

- Understand Linear Tape-Open technology and its unique architecture
- Learn about the IBM Ultrium drives and libraries
- Updated for Ultrium LTO 2 products

Charlotte Brooks
Carsten Krax
Tony Rynan
Josef Weingand

Redbooks

ibm.com/redbooks

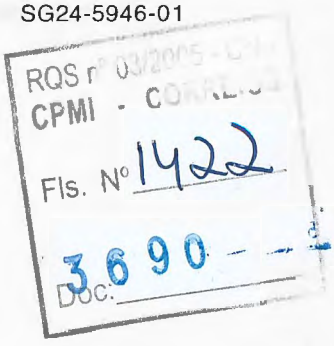
Fls. Nº 1421
3690
Doc:

International Technical Support Organization

The IBM LTO Ultrium Tape Libraries Guide

June 2003

SG24-5946-01



Note: Before using this information and the product it supports, read the information in "Notices" on page xvii.

Second Edition (June 2003)

This edition applies to the IBM TotalStorage Ultrium Tape Drive 3580, IBM TotalStorage Ultrium Tape Autoloader 3581, IBM TotalStorage Ultrium Tape Library 3582, IBM TotalStorage Ultrium Scalable Tape Library 3583, and IBM TotalStorage UltraScalable Tape Library 3584.

© Copyright International Business Machines Corporation 2000, 2003. All rights reserved.
Note to U.S. Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures xi

Tables xv

Notices xvii
Trademarks xviii

Preface xix
The team that wrote this redbook xix
Become a published author xxi
Comments welcome xxii

Summary of changes xxiii
June 2003, Second Edition xxiii

Chapter 1. Introduction to Linear Tape-Open (LTO) 1
1.1 The LTO organization 2
1.1.1 Open licensing and manufacture 3
1.1.2 License packages 4
1.1.3 Compliance verification 5
1.2 LTO standards 5
1.2.1 Ultrium tape formats 5
1.2.2 LTO core technology 6

Chapter 2. LTO technology 9
2.1 Interleaved recording 10
2.1.1 Servo tracks 10
2.1.2 Data tracks 13
2.1.3 Linear density 16
2.2 Data compression 16
2.3 Tape cartridge 18
2.3.1 Metal particle medium 20
2.3.2 Cartridge memory (LTO-CM) 20
2.3.3 Barcode label 22
2.3.4 Volume label format 23
2.3.5 Write protect switch 24
2.3.6 Cleaning the cartridge 24
2.3.7 Cartridge life 24
2.3.8 Cleaning cartridge 25

© Copyright IBM Corp. 2000, 2003. All rights reserved.

1423
Fls.
3690
Doc.

2.3.9 Cartridge handling 25
2.4 IBM LTO Ultrium common subassembly 28
2.4.1 Drive head 29
2.4.2 Data compression 30
2.4.3 Interfaces 31
2.4.4 Performance 35
2.4.5 Partial Response Maximum Likelihood (PRML) 36
2.4.6 IBM Ultrium 2: additional improvements 37
2.4.7 IBM Ultrium 1 and 2 compatibility 39
2.4.8 Operating the Ultrium drive 39
2.4.9 Reliability 41
2.4.10 Cleaning the drive 43
2.5 The IBM LTO Ultrium family of tapes and libraries 44
2.6 Multi-path architecture 46

Chapter 3. Tape storage market direction 49
3.1 Current tape products and technologies 50
3.1.1 Helical versus longitudinal 50
3.1.2 Tape reels (1/2-inch) 52
3.1.3 QIC 52
3.1.4 Digital Data Standard (4 mm) 54
3.1.5 The 8 mm format 56
3.1.6 Digital Linear Tape (DLT) 58
3.1.7 SuperDLT (SDLT) 62
3.1.8 IBM 3480 63
3.1.9 IBM 3490 63
3.1.10 IBM Magstar 3590 64
3.1.11 STK 9840 65
3.1.12 STK 9940 66
3.1.13 LTO Ultrium 66
3.1.14 Libraries 67
3.2 Current SAN technologies 68
3.2.1 SAN definition 70
3.2.2 Fibre Channel architecture 70
3.2.3 Topologies 71
3.2.4 Tape solutions in a SAN environment 71

Chapter 4. IBM TotalStorage Ultrium Tape Drive 3580 79
4.1 Model description 80
4.2 Feature codes 81
4.3 SCSI attachment 82
4.4 SCSI cabling 82
4.4.1 Cables 82

4.4.2 Interposers 83
4.4.3 SCSI length limitations 83
4.5 Upgrades 84
4.6 Environmental specifications 84
4.6.1 Physical dimensions 84
4.6.2 Operating environment 84
4.7 Host platforms and device drivers 84
4.7.1 Device driver installation 85
4.8 Storage applications 86
4.9 Performance considerations 86
4.10 Media 87
4.11 IBM 3580 Ultrium tape drive initial set-up 87
4.11.1 SCSI ID 87
4.12 Operator displays and buttons 88
4.12.1 Status light 88
4.12.2 Message display 89
4.12.3 The single-character display 89
4.12.4 Unload push button 90
4.13 Drive cleaning 90
4.14 Firmware upgrade 91

Chapter 5. IBM TotalStorage Ultrium Tape Autoloader 3581 93
5.1 Model description 95
5.1.1 Feature codes 96
5.1.2 Access mode 96
5.1.3 SCSI devices 97
5.1.4 Adding and removing cartridges 97
5.1.5 Operation 98
5.2 SCSI attachments 98
5.3 SCSI cabling 98
5.3.1 Cables 99
5.3.2 Interposers 99
5.3.3 SCSI length limitations 100
5.4 Upgrades and optional features 100
5.5 Environmental specifications 101
5.5.1 Physical dimensions 101
5.5.2 Operating environment 101
5.6 Host platforms and device drivers 101
5.6.1 Device driver installation 102
5.7 Storage applications 103
5.8 Performance considerations 103
5.9 Media 103
5.10 IBM 3581 initial setup 104

RQS nº 03.2005 - CN -
CPMI - CORREIOS
Fls. Nº 1424
3690
Doc:

5.10.1 SCSI ID 104
5.10.2 Element numbers 105
5.10.3 Operator displays and buttons 105
5.10.4 Message display 106
5.10.5 Drive status messages 107
5.10.6 Control buttons 108
5.10.7 Operating modes 110
5.11 Drive cleaning 111
5.12 Firmware upgrade 112

Chapter 6. IBM TotalStorage Ultrium Tape Library 3582 113
6.1 Model description 114
6.1.1 Tape drives 115
6.1.2 Cartridge storage 115
6.1.3 Barcode scanner 117
6.1.4 I/O station 117
6.1.5 Robotic system 117
6.1.6 Library control and operation 117
6.1.7 Operator panel 118
6.1.8 Maintenance 118
6.2 Feature codes 118
6.3 Physical attachments 119
6.4 SCSI cabling 120
6.4.1 Cables 120
6.4.2 Interposers 121
6.4.3 SCSI length limitations 121
6.5 Environmental specifications 121
6.6 Host platforms and device drivers 121
6.6.1 Device driver installation 122
6.7 Storage applications 123
6.8 Media 123
6.9 Installation and performance considerations 124
6.10 IBM 3582 initial set-up 124
6.10.1 SCSI ID 125
6.10.2 Identifying library location element numbers 125
6.11 Operator displays and buttons 125
6.11.1 Operator Panel 126
6.12 Library mode 128
6.13 Drive cleaning 128
6.14 Firmware upgrades 128

Chapter 7. IBM TotalStorage Ultrium Scalable Tape Library 3583 129
7.1 Model description 131

7.1.1 Tape drives 131
7.1.2 Cartridge storage 132
7.1.3 Barcode reader 132
7.1.4 I/O station 133
7.1.5 Robotic system 133
7.1.6 Library control and operation 133
7.1.7 Operator panel 134
7.1.8 Remote Management Unit 134
7.1.9 Library partitioning. 134
7.1.10 Multiple control paths 135
7.1.11 SAN Data Gateway Module 135
7.1.12 Maintenance 135
7.2 Feature codes 136
7.3 Physical attachments 137
7.4 Cabling 138
7.4.1 Fibre Channel cables 138
7.4.2 SCSI cables 139
7.4.3 Interposers 140
7.4.4 Terminator. 140
7.4.5 Cable length limitations. 140
7.5 Upgrades and optional features 141
7.5.1 Upgrade features 141
7.5.2 Optional features. 142
7.6 Environmental specifications. 142
7.7 Host platforms and device drivers. 143
7.7.1 Device driver installation. 144
7.8 Storage applications 144
7.9 Media. 145
7.10 Installation and performance considerations. 145
7.11 IBM 3583 initial set-up. 146
7.11.1 SCSI ID and LUN assignment. 146
7.11.2 Identifying library locations 147
7.11.3 Element numbers 150
7.12 Operator panel and RMU 151
7.12.1 Operator panel 151
7.12.2 RMU with TotalStorage Specialist. 154
7.13 Random access. 156
7.14 Drive cleaning 156
7.15 Firmware upgrades 157

Chapter 8. IBM TotalStorage UltraScalable Tape Library 3584 159
8.1 Model description 161
8.1.1 IBM 3584 Library Unit L32 161

2005 - CN - CORREIOS
FL. Nº 1425
3690
Doc:

8.1.2 IBM 3584 Expansion Unit D32 163
8.2 Library components 165
8.2.1 Tape drives 165
8.2.2 Library control systems: frame control assembly 167
8.2.3 Operator interface 170
8.2.4 Robotic cartridge accessor 172
8.2.5 Rail assembly 174
8.2.6 Library centric WWN convention 174
8.2.7 Control path failover 175
8.2.8 StorWatch 176
8.2.9 I/O station 177
8.2.10 Reliability 177
8.2.11 Service 179
8.2.12 Capacity 181
8.2.13 Adding and removing cartridges 185
8.3 Performance 186
8.4 Upgrades and optional features 188
8.4.1 Upgrade features 188
8.4.2 Optional features 189
8.5 Environmental specifications 189
8.5.1 Physical dimensions 189
8.5.2 Floor requirements 190
8.5.3 Operating environment 191
8.5.4 Power and cooling specifications 191
8.6 Host platforms and device drivers 192
8.6.1 Device driver installation 193
8.7 Storage applications 193
8.8 IBM 3584 initial setup 194
8.8.1 SCSI ID 194
8.8.2 Element number 194
8.9 Operator displays and buttons 196
8.10 Sequential versus random access 198

Chapter 9. IBM xSeries LTO tape products 199
9.1 IBM 3607-26X and 4560-SLX 200
9.1.1 Tape drives 202
9.1.2 Barcode reader 202
9.1.3 I/O station 202
9.1.4 Robotic system 203
9.1.5 Library control and operation 203
9.1.6 Operator panel 204
9.1.7 Maintenance 204
9.2 Library options 204

9.3 Physical attachments 205
9.4 Cabling 205
9.5 Environmental specifications 206
9.6 Storage applications 206
9.7 Media 206
9.8 Installation and performance considerations 207
9.9 Library features 207
9.9.1 Identifying library locations element numbers 207
9.10 Operator displays and buttons 208
9.10.1 Operator panels 208
9.10.2 Menu options 210
9.11 Library modes 210
9.12 Drive cleaning 210
9.13 Firmware upgrades 210

Chapter 10. LTO and iSeries considerations 213
10.1 iSeries support for IBM LTO Ultrium 2 214
10.2 BRMS and LTO tape libraries 215
10.3 iSeries resources 216
10.3.1 Configuration changes 218
10.4 OS/400 V5R1 restriction for multi-path architecture libraries 218
10.5 OS/400 V5R2 218
10.6 Tape drive sharing and management 220

Appendix A. LTO Ultrium tape media 223
Features available with IBM LTO hardware initial order 225
IBM TotalStorage Ultrium 1 Tape Drive 3580 225
IBM TotalStorage Ultrium 2 Tape Drive 3580 225
IBM TotalStorage Ultrium Tape Library 3582 225
IBM TotalStorage Ultrium 1 Scalable Tape Library 3583 226
IBM TotalStorage Ultrium 2 Scalable Tape Library 3583 227
IBM TotalStorage Ultrium 1 UltraScalable Tape Library 3584 227
IBM TotalStorage Ultrium 2 UltraScalable Tape Library 3584 228
IBM 3589 Ultrium 1 tape cartridge model number 228
Model description 229
Labelling service 229
IBM media business distributors and other suppliers 231

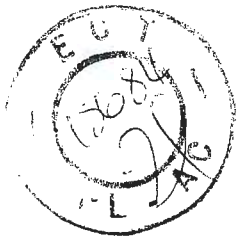
Abbreviations and acronyms 233

Related publications 235
IBM Redbooks 235
Other publications 235
Online resources 236

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1426
Doc 3690

How to get IBM Redbooks 237

Index 239



Figures

1-1 LTO Ultrium roadmap 2
1-2 LTO trademarks 5
1-3 IBM LTO Ultrium 1 and Ultrium 2 tape cartridges 6
2-1 Servo band position and nomenclature 11
2-2 Magnified servo band showing a pair of servo bursts 12
2-3 Encoding bits using the servo stripes within the servo bursts 13
2-4 Four data bands written between the servo tracks 14
2-5 Portion of data band showing Ultrium 1 track-writing sequence 15
2-6 LTO-DC block diagram 16
2-7 Ultrium cartridge view from top and rear 18
2-8 Ultrium cartridge view from top and front 19
2-9 Leader pin attached to the tape medium 20
2-10 Barcode label example 22
2-11 Turtle case 26
2-12 Double box 27
2-13 Correct leader pin placement 27
2-14 IBM LTO Ultrium common subassembly 28
2-15 Eight-element head (one set of heads shown) and servo elements . . . 29
2-16 Allocation of read and write heads for forward and reverse wrap 30
2-17 HD68 connector 34
2-18 VHDCI connector 34
2-19 IBM linear implementation of PRML encoding 37
2-20 Speed matching comparison: MB/sec 38
2-21 IBM Ultrium 1 and 2 compatibility 39
2-22 Front of subassembly showing operator panel indicators 40
2-23 Surface control guiding 42
2-24 Flat lap head 42
2-25 Statistical Analysis and Reporting System 43
2-26 The IBM Ultrium family of tapes and libraries 44
2-27 Conventional tape library vs. multi-path architecture 46
2-28 Redundant control paths to the library controller 47
2-29 IBM LTO tape library partitioned into three logical libraries 48
3-1 Tape reels, 1/2-inch 52
3-2 QIC cartridge 53
3-3 QIC head diagram 54
3-4 Helical-scan recording diagram 55
3-5 An 8 mm tape path 57
3-6 DLT tape path mechanism 59

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1427
Doc: 3690

3-7 DLT 2000 recording head design 60
3-8 DLT cartridge 60
3-9 DLT 2000/4000 linear recording format 61
3-10 DLT 7000/8000 tape head 61
3-11 Symmetric Phase Recording technology 61
3-12 Magstar 3590 tape cartridge 64
3-13 Magstar 3590 tape drive 65
3-14 STK 9840 tape cartridge 66
3-15 Overview of a SAN 69
3-16 IBM 3584 multi-path architecture 73
3-17 Electronic vaulting 75
3-18 Tivoli Storage Manager LAN-free backup 76
3-19 Tivoli Storage Manager server-free backup 77
4-1 IBM 3580 model L11/L13/L23 or H11/H13/H23 Ultrium tape drive 80
4-2 SCSI ID set-up example 88
4-3 Front view of the IBM 3580 tape drive 90
5-1 IBM TotalStorage Ultrium Tape Autoloader 3581 95
5-2 IBM 3581 cartridge slots 97
5-3 IBM 3581 front view 106
5-4 IBM 3581 message display 107
5-5 IBM 3581 operator panel 109
6-1 IBM TotalStorage Ultrium Tape Library 3582 114
6-2 IBM 3582 seven-slot magazines 116
6-3 IBM 3582 rear-mounted storage slots 116
6-4 IBM 3582 operator panel 126
6-5 IBM 3582 top-level menu options 127
7-1 IBM TotalStorage Ultrium Scalable Tape Library 3583 130
7-2 IBM 3583 storage columns: top view 148
7-3 IBM 3583-L72 location logical view 149
7-4 IBM 3583 front view, open door 150
7-5 IBM 3583 tape library operator panel 152
7-6 IBM 3583 flowchart of library functions 153
7-7 IBM 3583 soft key symbols 154
7-8 IBM 3583 operator panel: input field 154
7-9 IBM 3583 TotalStorage Specialist Web interface 156
8-1 IBM 3584 UltraScalable tape library L32 160
8-2 IBM 3584-L32 base frame view from front left 162
8-3 IBM 3584-D32 library expansion frame viewed from the right 163
8-4 IBM 3584 with 16 frames 164
8-5 IBM 3584 library showing the major library components 165
8-6 IBM 3584 LTO Ultrium tape drive assembly 166
8-7 Redundant drive power supply 167
8-8 IBM 3584 distributed control system 167

8-9 IBM 3584 distributed control system 168
8-10 Redundant medium changer controller 169
8-11 Frame controller assembly. 170
8-12 Operator panel 171
8-13 IBM 3584 accessor assembly 172
8-14 IBM 3584 Gripper. 173
8-15 Drive WWNs of an IBM 3584 175
8-16 Redundant control paths to the library controller 176
8-17 IBM 3584-L32 base frame showing cartridge slot components 182
8-18 IBM 3584-D32 expansion frame showing slot components 184
8-19 IBM 3584-L32 operator display 197
9-1 IBM 3607-26X Autoloader 200
9-2 IBM 4560-SLX Modular Tape Library 201
9-3 3607-26X front panel 208
9-4 4560-SLX touch screen front panel 209
10-1 Multiple-target support 219

468
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1428
Doc 3690

Tables

2-1 Data fields stored in the LTO-CM 21
2-2 SCSI terms and characteristics 33
3-1 Tape technology overview 51
3-2 DDS standards 56
3-3 Standards for 8 mm 58
3-4 DLT drive standards 62
4-1 IBM 3580 feature codes 81
5-1 IBM 3581 feature codes 96
5-2 IBM 3581 element numbers 105
6-1 IBM 3582 model summary 115
6-2 IBM 3582 feature codes 118
6-3 IBM 3582 element numbering 125
7-1 IBM 3583 model summary 131
7-2 IBM 3583 feature codes 136
7-3 IBM 3583 capacity upgrades 142
7-4 IBM 3583 storage slot coordinates 147
7-5 IBM 3583 element numbering 150
8-1 IBM 3584-L32 slot capacity without capacity expansion feature 183
8-2 IBM 3584-L32 slot capacity with capacity expansion feature 183
8-3 IBM 3584-D32 cartridge slot capacity 185
8-4 IBM 3584 bandwidth 187
8-5 Library performance 187
8-6 Power requirements for the IBM 3584 192
8-7 IBM 3584 tape drive element numbers 195
9-1 3607-26X Autoloader model summary 200
9-2 4560-SLX Modular Tape Library with Ultrium 1 drives 201
9-3 IBM 4560-SLX options 204
9-4 IBM 4560-SLX element numbering 207
9-5 IBM 3607-26X element numbering 208
9-6 Library manuals 211
A-1 Maximum number of media features for IBM 3583 Ultrium 1 226
A-2 Maximum number of media features for IBM 3583 Ultrium 2 227
A-3 Maximum number of media features for IBM 3584 Ultrium 1 228
A-4 Maximum number of media features for IBM 3584 Ultrium 2 228
A-5 Color specify feature codes for the IBM 3589 model 002 231
A-6 LTO Ultrium 1 and 2 available supplies and part numbers 231

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1429
3690

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1430
Fls. Nº
3690
Doc:

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
AS/400®
DFSMS/MVS®
DFSMShsm™
DFSMSrmm™
ESCON®
@server ™
@server™
FICON™
IBM®
ibm.com®
iSeries™
Magstar®
MVS™
Netfinity®
NetView®
OS/400®
pSeries™
Redbooks™
Redbooks (logo) ™
RS/6000®
ServerProven®
StorWatch™
Tivoli®
TotalStorage®
xSeries™

The following terms are trademarks of other companies:

Intel, Intel Inside(logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM Redbook presents a general introduction to Linear Tape-Open (LTO) technology and the implementation of corresponding IBM® products. As such it describes both general LTO technology specification and specific details of the unique design of IBM Ultrium tape drives and libraries.

In addition to the description of LTO, the reader will find technical information about each of the IBM Ultrium products, including generalized sections about SCSI and Fibre Channel connections, multi-path architecture configurations, and tape technology comparisons with market positioning.

This book is intended for anyone who would like to understand more about the general LTO technology specification and how it came about, as well as the IBM implementation of that specification. It is suitable for IBM clients, business partners, IBM specialist sales representatives, and technical specialists. Those with no background in computer tape storage products may need to reference other sources of information; in the interest of being concise, topics that are generally understood (in the opinion of the writers) are not covered in detail.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Charlotte Brooks is an IBM Certified IT Specialist and Project Manager for Storage Solutions at the International Technical Support Organization, San Jose Center. She has 13 years of experience with IBM in the fields of Storage, pSeries™ and AIX®. She has written 11 Redbooks™ and has developed and taught IBM classes on all areas of storage management. Before joining the ITSO in 2000, she was the Technical Support Manager for Tivoli® Storage Manager in the Asia Pacific region.

Carsten Krax is a Storage Specialist with the IBM Systems Sales Organization in Germany. He provides technical sales support for Open Systems Disk, Tape, and SAN solutions. Before he joined IBM two years ago, he worked from 1995 to 1998 as an System Administrator for an IBM Customer and from 1999 to 2001 as an ADSM/TSM and Storage Specialist for an IBM Business Partner. He holds a Diplom-Ingenieur (FH) degree in Electrical Engineering from the University of Applied Sciences in Dortmund, Germany.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1431
3690
Doc:

Tony Rynan is a senior software specialist at IBM Australia. He currently performs architectural and implementation services for IBM Global Services Australia throughout Southeast Asia. His areas of expertise include Tivoli Storage Manager, pSeries, SP, and SAN. He co-authored the redbook *Implementing IBM LTO in Linux and Windows*, SG24-6268.

Josef Weingand is an IT Specialist with the IBM Systems Sales Organization in Germany. He has seven years of experience providing technical support in IBM. He started as a customer engineer for Large Systems and worked 2 1/2 years as a Team Leader for the ITS European Support Center for Optical, Tape, and Tape Libraries. Now he is providing technical sales support for tape and backup solutions. He holds a Diplom-Ingenieur (FH) degree in Electronic Engineering from the Fachhochschule Kempten. He co-authored the Redbook *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

The team: Tony, Josef, Charlotte, and Carsten

Thanks to the following people for their contributions to this project:

The authors of the first edition of this book: Matthias Werner, Christina Coutts, Michel Marion, and Nelson Saavedra

Jon Tate, Emma Jacobs, Deanna Polm
International Technical Support Organization, San Jose Center

Betsy Thaggard
International Technical Support Organization, Austin Center

Nancy Coon, John Latimore, Dan Watanabe
IBM Tape Marketing, Tucson

Bob Bingham, Bobby Bohuslav, Michael DeGon, Brian Goodman, Lee Jesionowski, Dave Minch, Yun Mou, Steve Nunn, Bob O'Connell, Carol Pilch, MT Rincon, Robin Roberts, Carla Ruhl, John Sellars, Rob Wilson, Ray Yardy,
IBM Tape Architecture, Development, and Testing, Tucson

Rajesh Gurjar
IBM Systems Group, San Jose

Jo Lay
IBM Tivoli Storage Management Development, San Jose

Nancy Roper,
IBM iSeries™ Advanced Technical Support, Markham

Scott Maxson,
IBM iSeries Development, Rochester

David Turner,
IBM xSeries™ Tape Marketing, Raleigh

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1432
3690
Doc:

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  `ibm.com/redbooks`

- Send your comments in an Internet note to:

  `redbook@us.ibm.com`

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. QXXE Building 80-E2
  650 Harry Road
  San Jose, California 95120-6099

Summary of changes

This section describes the technical changes made in this edition of the book and in previous editions. This edition may also include minor corrections and editorial changes that are not identified.

Summary of Changes for *The IBM LTO Ultrium Tape Libraries Guide*, SG24-5946-01, as updated on June 9, 2003.

June 2003, Second Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

New information

- Ultrium 2 drives in existing LTO libraries
- New model, IBM® TotalStorage® Ultrium Tape Library 3582
- New functions (multi-path architecture, control path failover) for LTO libraries

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1433
3690
Doc:

1

Introduction to Linear Tape-Open (LTO)

The Linear Tape-Open (LTO) program is a joint initiative of IBM, Hewlett-Packard, and Seagate Technology. In 1997, the three technology provider companies set out to enable the development of best-of-breed tape storage products by consolidating state-of-the-art technologies from numerous sources, and in November of that year they produced a joint press release about LTO.

In the tape storage industry, Hewlett-Packard, IBM, and Seagate saw a common set of problems affecting customers in the midrange and network server areas. Multiple tape options are available, each offering certain strengths in terms of capacity, performance, data integrity, reliability, and cost, but no single option appears to meet all of these customer needs effectively. The LTO technology objective, therefore, was to establish new open-format specifications for high-capacity, high-performance tape storage products for use in the midrange and network server computing environments, and to enable superior tape product options.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1434
3690
Doc:

1.1 The LTO organization

The two principal Web sites for marketing, technical, and licensing detail for the Linear Tape Open program are

`http://www.lto-technology.com`
`http://www.ultrium.com`

Two LTO formats (Ultrium and Accelis) were originally introduced in 1997, and licenses for the new technology were made available. Since then, the Accelis format has not been actively pursued by manufacturers because it is apparent that the Ultrium format meets market needs. The three LTO sponsoring companies (IBM, Hewlett-Packard, and Seagate) also took steps to protect customer investment by providing a four-generation roadmap, shown in Figure 1-1, and establishing an infrastructure to enable compatibility between products. At the time of writing, LTO generations 1 and 2 are available.

LTO Ultrium Road Map

	Generation 1	Generation 2	Generation 3	Generation 4
Capacity (Native)	100GB	200GB	400GB	800GB
Transfer Rate (Native)	10-20MB/s	20-40MB/s	40-80MB/s	80-160MB/s
Media	Metal Particle	Metal Particle	Metal Particle	Thin Film

Figure 1-1 LTO Ultrium roadmap

Important: Hewlett-Packard, IBM, and Seagate reserve the right to change the information in this migration path without notice.

The LTO Ultrium compatibility investment protection is provided based on the following principles:

- An Ultrium drive is expected to read data from a cartridge in its own generation and at least the two prior generations.

– An Ultrium drive is expected to write data to a cartridge in its own generation and to a cartridge from the immediate prior generation in the prior generation format.

Existing compatibility between the available Ultrium 1 and Ultrium 2 media is discussed in 2.4.7, "IBM Ultrium 1 and 2 compatibility" on page 39.

The three technology provider companies (HP, IBM, and Seagate) have all made significant contributions of time and expertise to the definition of the LTO format specifications. All have deep knowledge of customer needs and have provided expert knowledge and engineering skill in the critical areas of magnetic recording technology, mechanism design, media materials, and cartridge design. This cooperative process has created stronger LTO format definitions than any of the individual companies would have developed working alone.

1.1.1 Open licensing and manufacture

To answer industry calls for open tape format specifications, LTO format specifications have been made available to all who wish to participate through standard licensing provisions. More than 25 companies, including HP, IBM, and Seagate, have become LTO technology licensees. The licensees include an impressive array of worldwide storage industry leaders such as:

- Accutronics Inc.
- ADIC
- Advanced Research Corp.
- Alps Electric Co. Ltd.
- Certance
- EDP/Colorflex
- EMag Solutions
- EMTEC Magnetics GmbH
- Exabyte Corporation
- Fuji Photo Film Company Ltd.
- Fujitsu Ltd./FCPA Intellistor
- Hewlett-Packard Co.
- Hi/fn
- IBM Corp.
- Imation Corp.
- M4 Data Ltd.
- Matsushita Electric Industry
- Maxwell
- Mitsumi Electric Co. Ltd.
- Mountain Engineering II Inc.
- NEC Corp.
- Otari Inc.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1435
3690
Doc:

- Ontrack Data International
- Overland Data, Inc.
- Phillips Semiconductor Gratkorn
- Plasmon IDE Inc.
- Quantegy Inc.
- Seagate Corporation
- Sony Corp.
- Tandberg Data
- TDK Corp.
- Verbatim Corp.

In attracting these other industry leading companies, LTO program technology and LTO specified products (tape drives and tape storage cartridges) will reach the market from multiple manufacturers, not just the technology provider companies. This is critical to meeting an open market objective and is accomplished through open licensing of the technology.

1.1.2 License packages

Three combinations of packages are available for potential licensees:

- *Ultrium Specification Document* provides the opportunity to review Ultrium format specification with a minimal investment and is suitable for those companies interested in a feasibility investigation.
- *Ultrium Tape Cartridge License Package* is for those companies interested only in designing Ultrium tape cartridges.
- *Ultrium Tape Mechanism License Package* enables the licensee to design Ultrium tape drive mechanisms.

Each license package contains one or all of the following types of documents:

- *Format specification documentation*, which provides the technical information about the format necessary to develop mechanisms and cartridges that interchange between products of the same format.
- *License documentation*, which provides additional technical information about tolerance interdependencies and interchange verification testing, and also presents a conceptual overview of the design.

- The *trademark style guide*, which describes the use of the Ultrium trademarks and logos (Figure 1-2 on page 5).

Figure 1-2 LTO trademarks

1.1.3 Compliance verification

The technical strategy for accomplishing format compliance verification among the licensees has been defined, and an independent Compliance Verification Entity (CVE) has been selected. In an effort to promote interchangeability of tape cartridges, the TPCs are enlisting the services of a third-party verification test company to perform specification compliance verification testing. These tests will be required annually for all companies that use the logo.

The objective of the compliance testing is to test only the ability to produce and/or read and write Ultrium cartridges that meet the format specifications. It is not an objective of this format compliance testing to evaluate Ultrium drive quality, MTBF, physical form factor, or other parameters not directly related to the LTO program formats and interchangeability. LTO program licensees have wide latitude to establish their own mechanical, electrical, and logic designs to meet the format specifications. These factors will not be tested as part of the compliance verification process.

For more details about the packages, documentation, or licensing, refer to the LTO Web site:

`http://www.lto-technology.com`

1.2 LTO standards

LTO Technology was originally developed for two open tape format specifications: Accelis and Ultrium. The Accelis format (fast-access) is not being developed as the Ultrium format provides adequate fast-access performance.

1.2.1 Ultrium tape formats

Figure 1-3 on page 6 shows the IBM Ultrium cartridges, which can be distinguished by color: The first generation IBM cartridge is black, and the second generation (Ultrium 2) cartridge is purple.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1436
3690
Doc:

complete the round trip. For the next round trip, the heads are again indexed to a new position over a new group of eight tracks.

Because track densities are high, and because the tape is subject to some lateral movement as it is moved, it is critical for performance and data integrity that the read/write heads are always positioned precisely over the correct tracks. This is accomplished through a technique called timing based servo. This technique makes it possible to use high track densities, now and in the future, without changing the format of the media, and it provides the ability to read data, even with media imperfections.

In the LTO system, electronic signals are generated through the real-time reading of servo data bands that are prerecorded on the LTO tape. These signals enable the servo system to dynamically control the positioning of the read/write heads across the width of the tape. Similar magnetically based, track-following servo systems are proven in tens of thousands of tape drives in use today such as the IBM Magstar® High Performance Tape Drive.

The LTO formats also utilize advanced error correction codes for data integrity. These systems are designed to automatically correct most cross-track errors and provide data correction even if a full track is lost. Data is further protected by demarcation of bad areas of the tape (for example, where servo signals are unreliable) and through dynamic rewriting of bad blocks. Cartridge memory is embedded in the LTO cartridges. A non-contacting radio frequency module, with non-volatile memory capacity of 4096 bytes, provides for storage and retrieval of cartridge, data positioning, and user-specified information.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1437
3690
Doc:

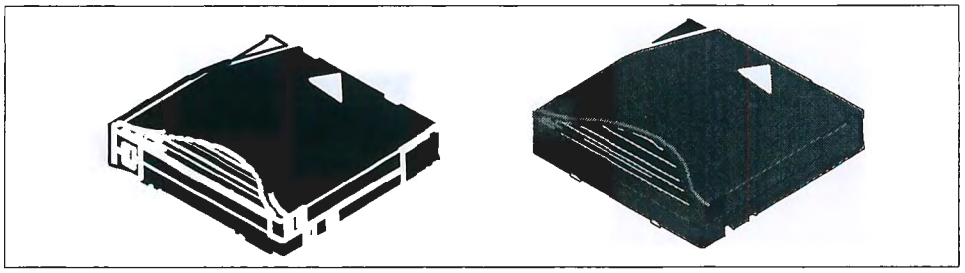


Figure 1-3 IBM LTO Ultrium 1 and Ultrium 2 tape cartridges

The Ultrium tape format specification is the implementation of LTO optimized for high capacity and performance with outstanding reliability, in either a stand-alone or an automated environment. The Ultrium cartridge uses a larger single-reel design (Figure 1-3) and 1/2-inch tape to provide ultra-high storage capacity. The tape is extracted from the cartridge by the tape drive through a leader pin, and wound onto a take-up reel contained within the drive itself. This design is focused on customer requirements for very high capacity and performance, and is ideally suited for backup, restore, and archive applications. Ultrium drive technology is intended to meet the needs of the enterprise on a roadmap, or migration path, that extends well into the future. The Ultrium tape format establishes a new benchmark for large volume backup and archive.

1.2.2 LTO core technology

Multi-channel linear serpentine recording is at the core of the LTO formats. It enables an optimum balance of reliability and data integrity, performance, and high capacity. In the LTO recording format, data is written in tracks that run down the length of the tape.

The Ultrium format records either 384 tracks (Ultrium 1) or 512 (Ultrium 2) across the half-inch of tape width. This linear recording format has a *serpentine* characteristic. The drive mechanism will make multiple passes from the beginning of the tape to the end of the tape and back in order to read or write the full capacity of the cartridge. In the Ultrium 1 format, the 384 tracks are split into four bands of 96 tracks each. In Ultrium 2 format, the 512 tracks are split into four bands of 128 tracks each. Data is written to the innermost bands first, to provide protection to the data recorded earliest in the process, by writing it in the center, the most physically stable area on the tape. Data is also verified as it is written. On pass one of a round trip down the length of the tape and back, eight tracks are read, or written, concurrently. At the end of the tape, pass two of the round trip starts. The read/write heads are indexed and positioned over eight new tracks, and the tape reverses direction back toward the beginning of the tape to

2

LTO technology

This chapter covers the LTO format specifications in general terms, including first and second generation Ultrium. The information referring to the data cartridge, the format in which data is written, elements of the drive specification relating to that format, and the compression algorithm description, are all part of the documented LTO specification. This kind of information will be applicable to all LTO manufacturers' product offerings in order to ensure cartridge interchangeability.

The information relating to the LTO Ultrium drive given in this chapter relates to the IBM LTO Ultrium drive, and may not be the same as those from other manufacturers in regard to such features as data rate and reliability.

This chapter also gives an overview of the IBM product offerings, which are covered in detail in later chapters.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1438
3690
Doc:

2.1 Interleaved recording

The drive uses an interleaved, serpentine, longitudinal recording format. The first set of eight data tracks is written from near the physical beginning of the tape to near the physical end of the tape. The head then repositions to the next set of tracks for the return. This process continues until all tracks are written and the tape is full.

The format of the recording of the data and servo tracks is defined as part of the LTO specification in order to meet the requirement for interchange between different manufacturers implementations.

2.1.1 Servo tracks

Servo tracks (also called bands) enable accurate positioning of the tape drive head over the data track, ensuring that the head does not stray onto an adjacent track. They are necessary to support high-data densities on the tape where the tracks are very close together. The servo bands are written at time of cartridge manufacture, before the cartridge is usable for data storage and retrieval.

Servo tracks are like lane markings on a multi-lane highway. Imagine how difficult it would be to drive on a highway without any lane markings. Lane markings help by positioning you on the lane, just as servo tracks support the drive recording head to position on the data tracks.

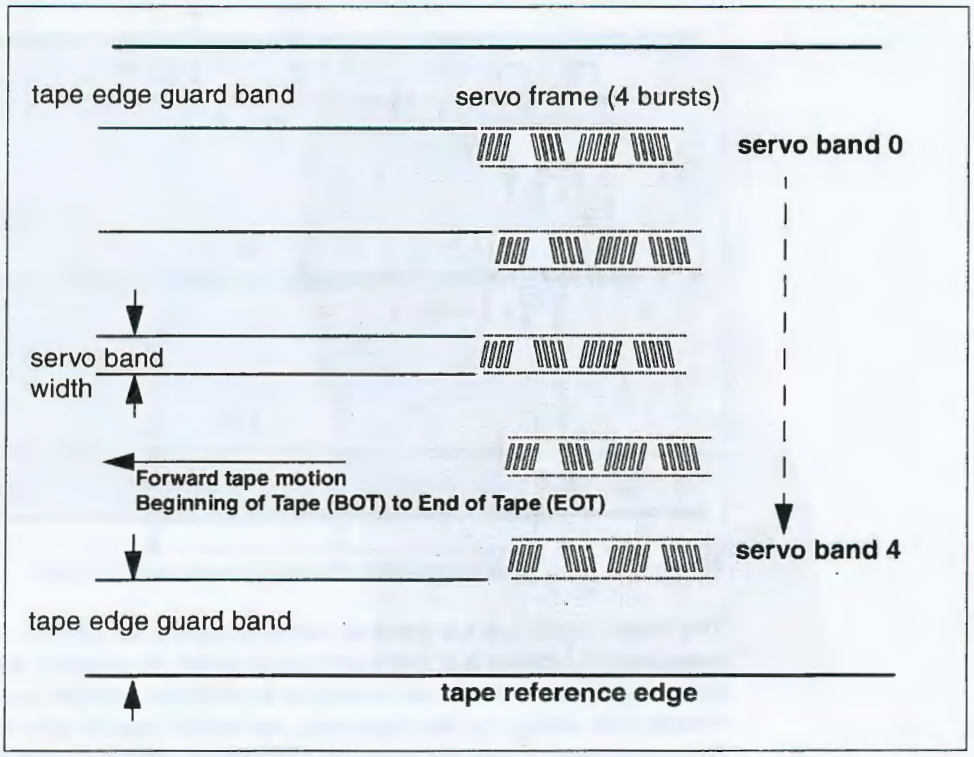


Figure 2-1 Servo band position and nomenclature

As shown in Figure 2-1, five servo bands, numbered 0 through 4, make up the servo tracking mechanism on the LTO Ultrium tape. They are each located at specific distances from the tape reference edge[1]. Within the servo bands are servo stripes, groups of which make up servo bursts. Four servo bursts make up a servo frame; the first two bursts (as written in the forward tape-motion direction) contain five servo stripes, and the second two bursts contain four servo stripes.

Track following

Each pair of servo bursts is at an angle to each other, and the servo heads move such that they keep a constant value for the distance between the bursts. In this way the servo is able to follow a straight line within the servo band; any small deviation away from the correct path causes a variation (plus or minus) in the gap between the bursts (see Figure 2-2 on page 12). Provided that the servo head element follows a straight line along the servo band, then the distance "x" shown in the figure remains constant. Two servo bands are used simultaneously to provide two sources of servo information for increased accuracy.

[1] The reference edge of the tape is the bottom edge when viewing the recording side of the tape with the hub of the tape to the observer's right, as shown in Figure 2-1.

RQS nº 03/2005 - CN - CPMT - CORREIOS
1439
Fls. Nº
3690
Doc:

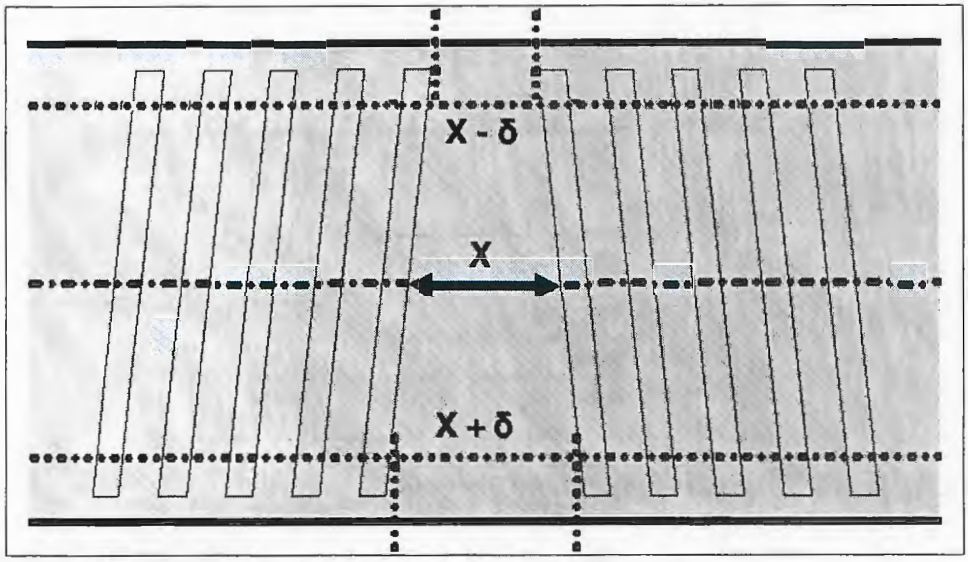


Figure 2-2 Magnified servo band showing a pair of servo bursts

The format specifies six nominal servo positions for Ultrium 1 and eight servo positions for Ultrium 2 within each servo band. In addition, the servo head is made up of two servo head elements to address a single servo band. This means that, using the two elements, the servo head is able to reposition within the servo band for the six (Ultrium 1) or eight (Ultrium 2) forward and reverse data wraps within each data band (Figure 2-5 on page 15). The distance between each servo position corresponds to the distance apart that the data tracks are written. For further information about the drive head and elements, see 2.4.1, "Drive head" on page 29 and Figure 2-15 on page 29.

This technology can be very finely tuned and is capable of supporting very high track densities using the same servo tracks because the currently used and defined six/eight nominal positions are basically definitions of six/eight different "x distances" between servo bursts (see Figure 2-2) and not a fixed servo track. By defining additional "x distance" positions, it is possible to increase the number of tracks on an LTO Ultrium while still using the same technology. With this technology, LTO is also able to satisfy the compatibility aspects as described in 1.1, "The LTO organization" on page 2. The Ultrium 2 drives have to use the six defined "x distances" on the Server tracks to read and write in Ultrium 1 Format.

Longitudinal positioning

The LTO servo band is designed not only for track following but also for recording the longitudinal position (LPOS). The absolute location down the length of the tape and the manufacturer data are recorded in LPOS "words," approximately

every quarter-inch (.7 cm) along the tape. The LPOS word consists of symbols constructed from bit sequences (ones and zeros); these bits are encoded within the servo frames.

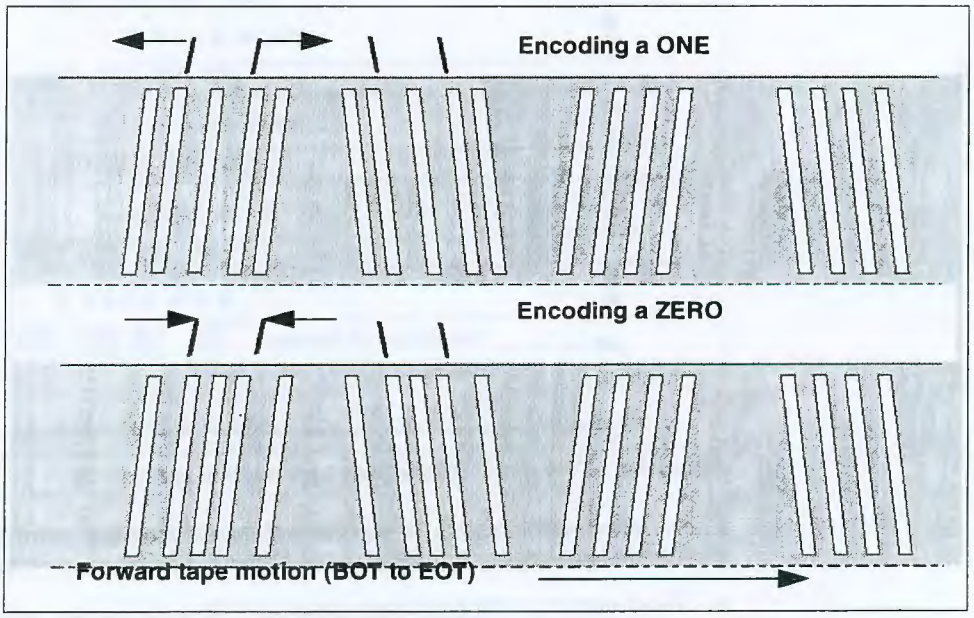


Figure 2-3 Encoding bits using the servo stripes within the servo bursts

Each servo frame encodes one bit using the first pair of servo bursts. When servo stripes 2 and 3 (out of the five) are shifted inward (see Figure 2-3), this encodes a zero; when servo stripes 2 and 3 are shifted outward, this encodes a one. The LPOS word contains 36 bits and thus has a length of 36 servo frames.

Each of the 5 servo bands on the tape may be uniquely identified by the relative positions of the frames down the tape, in adjacent servo bands. The offset of the frames between servo band n and servo band $n+1$ are specific to each servo band (0 and 1, 1 and 2, 2 and 3, or 3 and 4). Thus the drive can move the head directly from the physical beginning of the tape to a specific logical position for reading or writing.

2.1.2 Data tracks

The area between adjacent servo bands is a data band. There are four data bands numbered 2, 0, 1, and 3, where data band number 2 is nearest the reference edge of the tape and data band 3 is farthest away, as in Figure 2-4 on page 14. The data bands are written in sequence beginning with 0 (in the center of the tape) and ending with 3.

DOC 3690 - CN -
CPMI - CORREIOS
Fls. Nº 1440
Doc: 3690

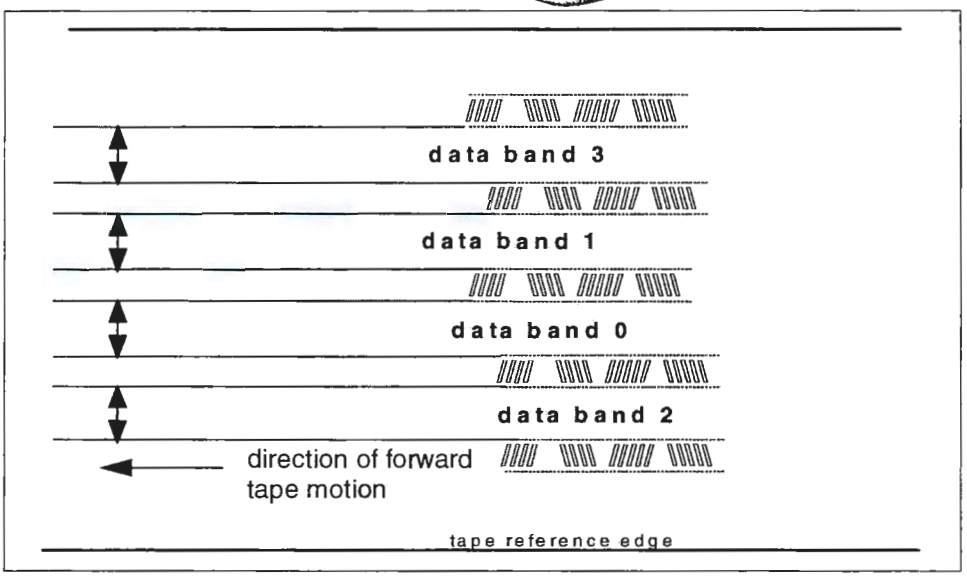


Figure 2-4 Four data bands written between the servo tracks

Each data band consists of numbers of tracks that are recorded eight tracks at a time from one end of the tape to the other in the following way:

- The head is positioned over data band 0, and the first set of eight tracks is written from the physical beginning of the tape to the physical end.
- The head physically repositions (using a different servo position within the same servo bands) and switches electronically[2] to a second set of eight write elements in order to write eight tracks in the reverse direction back to the physical beginning of the tape.
- The head physically repositions again, and, switching back to the first set of write elements, writes another set of eight tracks to the physical end of the tape.
- The head continues to switch and index in this manner until all 96 tracks are written and the head is back at the physical beginning of the tape.
- The head moves to data band 1 to continue writing the data.

For Ultrium 1, 96 data tracks coexist in one data band. For Ultrium 2, there are 128 data tracks in one data band.

A group of tracks recorded concurrently in the physical forward or the physical backward direction is called a *wrap*. Wraps recorded while the tape is moving from BOT to EOT are forward wraps; wraps recorded while the tape is moving

[2] See 2.4.1, "Drive head" on page 29 for more information about electronic head switching.

from EOT to BOT are reverse wraps. The wraps are recorded in a serpentine fashion, as described: a forward wrap, then a reverse wrap. They are numbered sequentially in the order that they are processed, starting with wrap 0. Thus, for Ultrium 1 six forward wraps and six reverse wraps make up a data band. For Ultrium 2, eight forward and eight reverse wraps make up a data band. The individual tracks within a wrap are interleaved with tracks from other wraps; in other words, adjacent tracks are not part of the same wrap. (See Figure 2-5.)

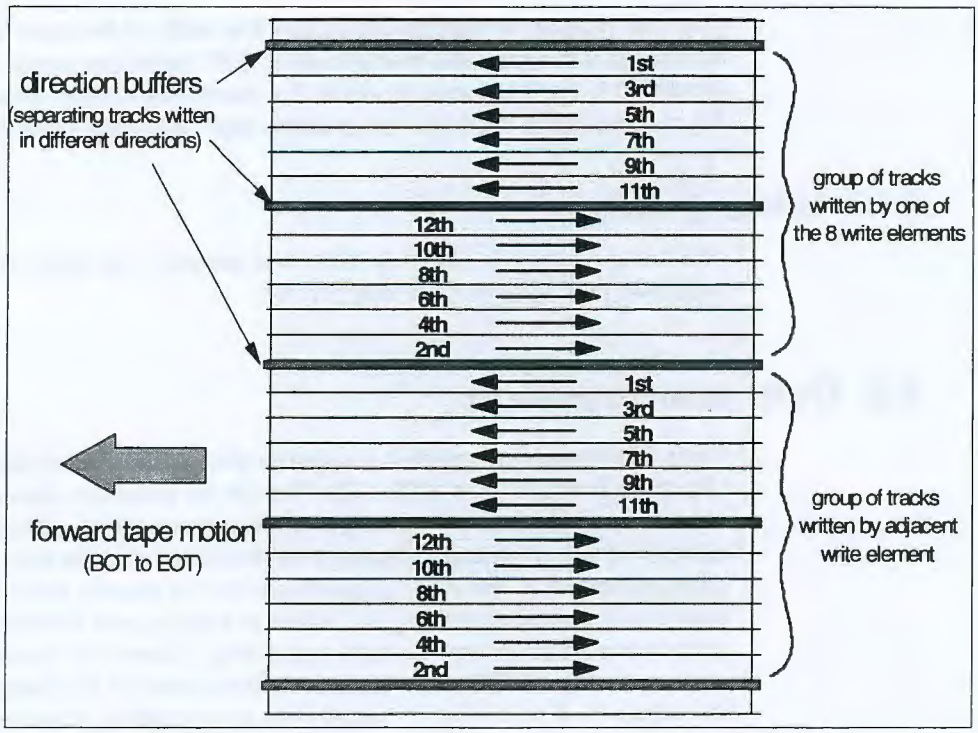


Figure 2-5 Portion of data band showing Ultrium 1 track-writing sequence

This figure expands on Figure 2-4 on page 14 to illustrate the sequence in which the tracks are written. One data band is magnified[3] to show an area written by two adjacent write head elements (from the total of eight); this is one quarter of the width of the data band. You can see that the tracks are written in an inward spiral (serpentine) manner; the first and second tracks are farthest away from one another while the 11th and 12th tracks are adjacent to one another.

[3] Refer to 2.4.1, "Drive head" on page 29, and Figure 2-15 on page 29, to see the structure of the eight-element head.

RCS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1441
3690
Doc:

The space between tracks written in opposing directions is called a direction buffer. This space is designed to minimize magnetic interference between tracks written in opposite directions (cross-track interference).

Read/verify elements are built into the tape head in the drive. The data is written by the write elements and then immediately passes the read/verify elements and is checked for errors. If any errors are found, the block of data is rewritten farther down the tape.

The total number of data tracks across the width of the tape is 384 for Ultrium 1, numbered 0 through 383. For Ultrium 2, 512 tracks are used. Track numbering is unrelated to the sequence in which the tracks are written: data track 383/512 is the closest to the reference edge of the tape, and data track 0 is farthest away.

2.1.3 Linear density

The linear density for LTO 1 is 4880 bits per mm. The linear density was improved for LTO 2 to 7398 bits per mm.

2.2 Data compression

The LTO Consortium created a superior data compression technique know as LTO Data Compression (LTO-DC). Though an excellent data compression algorithm, ALDC (adaptive lossless data compression), already exists, ALDC function is not optimized for incompressible data such as encrypted or previously compressed data. For incompressible data, it is usually best not to apply any data compression algorithm, but rather to simply pass the input data out to the compressed data stream directly (pass-thru). Given the variations in data, there are times when ALDC is desirable and times when a simple pass-thru is better. For instance, if using ALDC-based data compression, it would be best if all segments of incompressible data were to be recorded without expansion by using a pass-thru technique instead. Figure 2-6 is a block diagram illustration of the LTO-DC data compression technique using the two schemes.

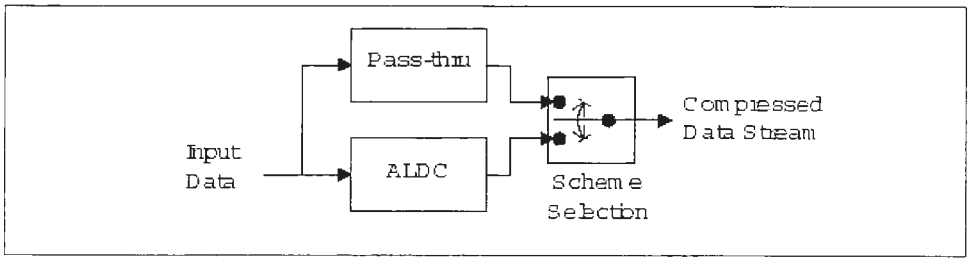


Figure 2-6 LTO-DC block diagram

Note that no standardization of when to scheme swap when compressing data was specified by LTO-DC. LTO-DC was approved by ECMA as SLDC [streaming lossless data compression] standard, as explained at:

`http://www.ecma-international.org/publications/standards/ECMA-321.htm`

Because no standardization is specified, all vendor implementations may do scheme swapping differently. What is specified and tested is that the resultant compressed data stream is decompressible by the defined set of LTO-DC rules. This enables interchange between drives from the three companies. Each vendor's Ultrium drive has been shown to be able to read and decompress the LTO-DC streams of the others.

Embedded codewords

LTO-DC uses embedded codewords to enable swapping between the two schemes. ALDC is referred to as Scheme 1, and pass-thru is referred to as Scheme 2. Both methods are used. However, only one is used to output any given data byte, though different bytes in a record might be output in different schemes. Thus, if a given record begins with compressible data it can be output in Scheme 1, and if the nature of the data changes inside of the record and it becomes incompressible (as embedded control data or an array of incompressible data), a scheme swap can be performed to allow outputting the incompressible data in Scheme 2. Similarly a scheme swap can be performed to revert to Scheme 1 if the data becomes compressible again. A scheme swap is denoted in the compressed data stream via one of four embedded codewords. As an example, one 13-bit codeword basically means all following data is to be decompressed as Scheme 1 until another scheme swapping codeword is encountered. Embedded codewords are also used to delineate record boundaries and filemarks. Having record boundaries demarked within the output compressed data stream, rather than by pointers maintained in a separate directory table, has a number of advantages. First, from a storage point of view, it is more efficient as it enables greater capacity. Second, the insertion of these codewords enables higher-speed data streaming because they can be managed by the compression engine without microprocessor involvement. Both of these features are especially useful for small records. Typically, backup applications will send 512-byte, 4-KB, 32-KB, or 256-KB records to a backup tape drive. For small records such as 512 bytes, the improved format efficiency of the embedded control is substantial. By reducing required microprocessor involvement it allows superior transfer rates to the drives. This is why LTO tape drives offer high capacity tape backup, as well as drive transfer rates far better than other midrange backup tape drives—and are superior even to some costly, high-end tape drives.

The ability to swap between ALDC and a pass-thru mode gives a tape drive the power to automatically adapt to the incoming data stream.

RQS nº 03.2005 - CN - CPMI - CORREIOS
Fls. Nº 1442
3690
Doc:

2.3 Tape cartridge

The Ultrium cartridge is a single-reel cartridge. This means the whole tape is wrapped around a single reel when the cartridge is not loaded in a drive. During the loading process, the threader of the drive catches the leader pin of the tape and threads it through the drive and the machine reel. During the read/write process the tape is stored on the machine reel and the cartridge.

Two views of the tape cartridge are shown in Figure 2-7 and Figure 2-8 on page 19.

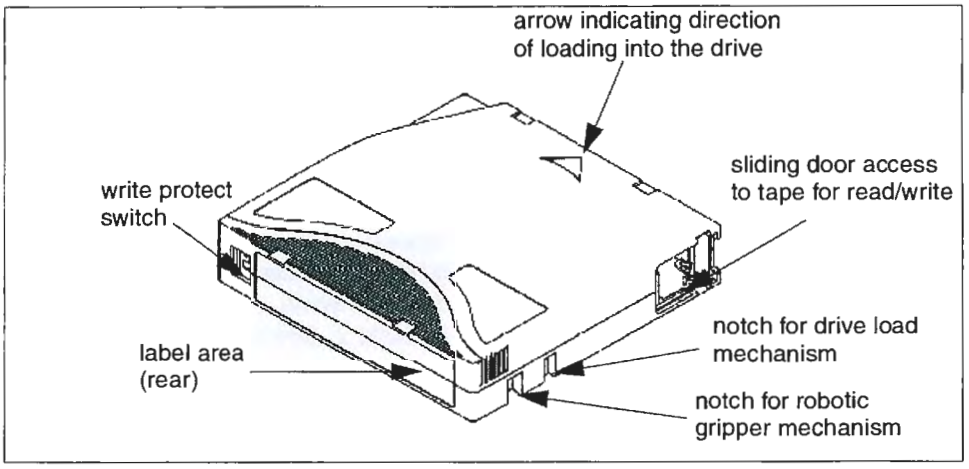


Figure 2-7 Ultrium cartridge view from top and rear

The cartridge is approximately 10.2 cm long, 10.5 cm wide, and 2.2 cm high (approximately 4 x 4.16 x 0.87 inches). The cartridge contains 1/2-in (12.6 mm), metal-particle tape with a highly dense recording area. The Ultrium 1 spec describes four types of cartridges, each with a different tape length and, therefore, capacity. At this time, only one cartridge type is generally available, with a tape length of 610 m (2000 feet) providing 100 GB of native data and 200 GB of compressed data (assuming 2:1 compression). There is only one standard Ultrium 2 cartridge type and hence only one tape length of 610m (2000 feet). The native capacity of the Ultrium 2 cartridge is 200 GB (400 GB compressed assuming 2:1 compression).

Figure 2-8 on page 19 shows some of the components of the cartridge.

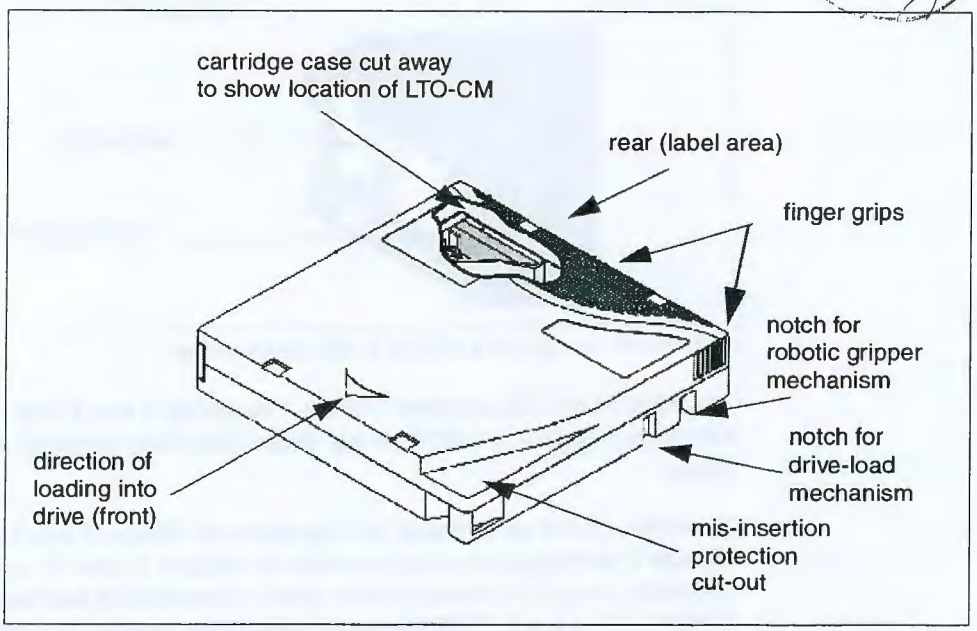


Figure 2-8 Ultrium cartridge view from top and front

The labelled parts are:

- Grips: Molded areas on the cartridge casing designed as finger grips for manual loading.
- Label area: Located at the designated area at the rear of the cartridge where the adhesive bar code label is applied.
- Sliding door: Cartridge door (shown in Figure 2-7 on page 18) that protects the tape from contamination whenever the cartridge is out of the drive. Behind the door, the tape is threaded onto a leader pin (shown in detail in Figure 2-9 on page 20), which is used to pull the tape from the cartridge for use. A locking mechanism prevents the media from unwinding when the cartridge is not located in the drive.
- Notches: Two sets of moulded notches in the cartridge casing located on the sides near the rear. The first pair enables the robotic gripper to pull the cartridge out of the drive mouth once the cartridge has been unloaded; the second pair enables the drive to grip the cartridge and pull it into the loading position inside the drive.
- Mis-insertion protection: A cut-out in the front side of the cartridge casing that prevents the cartridge from being inserted into the drive in the wrong orientation. This feature prevents the use of unsuitable cartridges of similar, but not identical, construction.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
1443
Fls. Nº
3690
Doc:

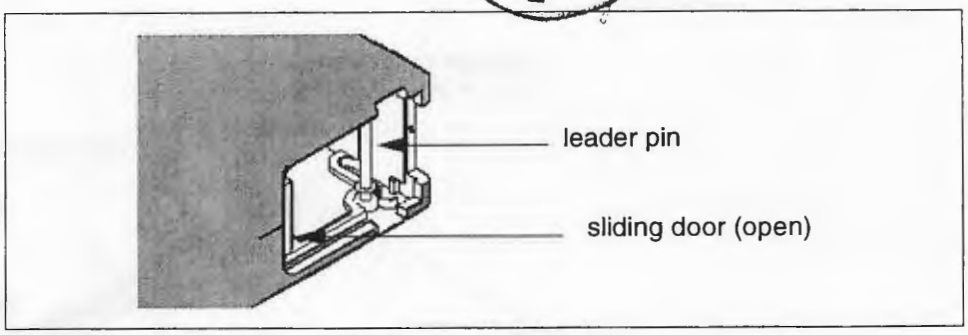


Figure 2-9 Leader pin attached to the tape medium

The shell of an IBM branded Ultrium 1 cartridge is black and of an Ultrium 2 cartridge is purple, providing easy visual distinction between the two media types.

Even though the servo tracks are the same on Ultrium 1 and Ultrium 2 cartridges, Ultrium 2 cartridges are required with an Ultrium 2 drive to achieve Ultrium 2 capability. More information about media compatibility between Ultrium 1 and Ultrium 2 is in 2.4.7, "IBM Ultrium 1 and 2 compatibility" on page 39.

2.3.1 Metal particle medium

The metal particle tape medium consists of a transparent polyethylene base material with two coatings. On one side, the base has two fine coats of a strong yet flexible ferromagnetic material, dispersed in a suitable binder; this is the surface on which the data is written. The back surface is coated with a non-ferromagnetic conductive coating.

Metal particle media have high coercivity, which is a measure of their ability to retain their magnetic properties once the data is written to the tape; this is one of the factors in enabling a potentially longer shelf life than other media.

2.3.2 Cartridge memory (LTO-CM)

Information about the cartridge and the tape is written to the LTO-CM, which is a serial EEPROM with both read-only and rewriteable areas. It is housed inside the cartridge casing at the left rear (label side) corner as illustrated in Figure 2-8 on page 19, which shows the interior of the cartridge casing.

The LTO-CM has a capacity of 4096 bytes. It is used to hold information about that specific cartridge, the media in that cartridge, and the data on the media. A copy of this information is also kept in the first data set within the user data area, and is given the data set number zero.

Communication between the drive and the LTO-CM uses a contactless low-level radio frequency (RF) field generated (in the IBM implementation) by the drive. The LTO-CM is non-volatile storage updated using the RF field; it requires no additional power source. This type of technology has an expected shelf life of more than 30 years.

There are a number of distinct data fields within the LTO-CM, shown in Table 2-1. The fields align to 32-byte boundaries, as this is the defined block access size.

Table 2-1 Data fields stored in the LTO-CM

LTO-CM information	Read/write
LTO-CM manufacturer's data	Read-only
Tape label[a]	
Media manufacturer information	
Initialization data[b]	Restricted write capability
Cartridge status and tape alert flags	Read or write
Usage information	
Tape write pass	
Tape directory	
End-of-data information	
Mechanism related	
Application specific data[c]	
Vendor unique data	

a. This field contains information about the tape, including a 10-byte field with the tape serial number; it is a read-only area and does not contain the volume label, which could be changed if the tape is reinitialized.
b. This is a restricted-write field that is updated with changes when the tape is reinitialized.
c. This is a field for application data (such as the volume label) to be stored in the CM. However, currently there is no SCSI function available to support writing to that area.

Although transparent to the user, keeping this kind of information enhances the efficiency of the drive and cartridge. Data and block locations are stored in memory; for example, the end-of-data location is stored, so that when the tape is next loaded, the drive can use the fast locate function to move directly to the recording area and begin recording. Storing data about the age of the cartridge, how many times it has been loaded, and how many errors it has accumulated

ROS nº 03/2005 - CN - CPMI - CORREIOS
1444
Fls. Nº
Doc: 3690

aids in determining the reliability of the cartridge. It is of particular value if this data is stored with the cartridge itself, so that whenever it is mounted on any host system, the history is accessible.

This is not the first tape product where information has been kept on the cartridge; however, previously it has been written onto the tape medium itself in a non-user-accessible portion of the tape before the beginning-of-tape (BOT) marker, for example, as in the IBM 3590 tape drive.

2.3.3 Barcode label

Each data and cleaning cartridge processed by an Ultrium tape library should bear a barcode label. (This is mandatory for libraries that have an installed barcode reader such as the IBM 3584.)

The label, as shown in Figure 2-10, contains a human-readable volume serial number or volume label, and a machine-readable barcode.

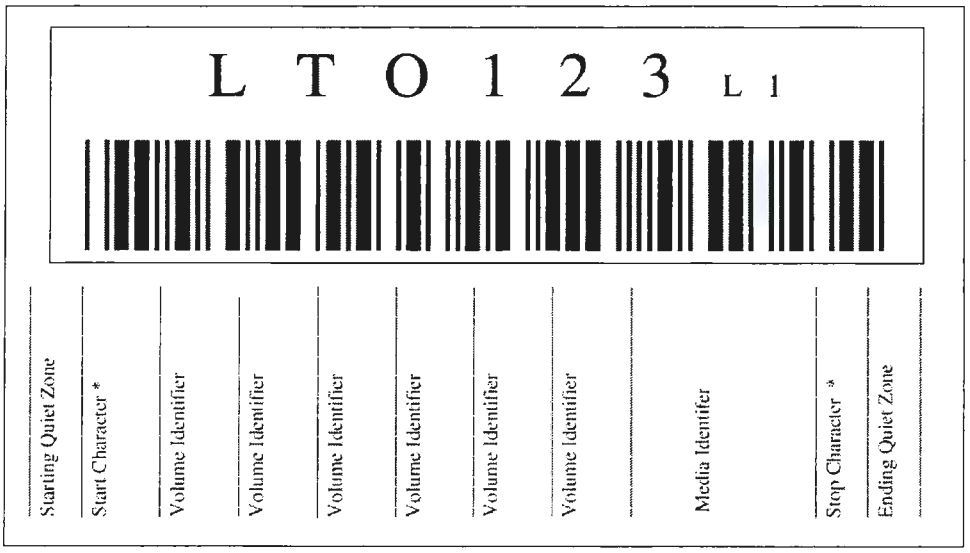


Figure 2-10 Barcode label example

The bar code format is:

- Quiet zones (at each end of the bar code)
- A start character (indicating the beginning of the label)
- A six-character volume label

- A two-character cartridge media-type identifier (L1 or L2), which identifies the cartridge as an LTO cartridge ('L') and indicates that the cartridge is the first ('1') or second generation ('2')
- A stop character (indicating the end of the label)

When read by the library's barcode reader, the barcode identifies the cartridge's volume label to the tape library. The barcode volume label also indicates to the library whether the cartridge is a data, cleaning, or diagnostic cartridge.

Tape cartridges are often supplied with the labels already attached, or you can attach a label yourself. Operators must handle the cartridges and barcode labels in accordance with the instructions in the operator guides supplied with the products. You must ensure that labels are removed cleanly, reapplied carefully, in good condition, and not obscured or damaged. The Ultrium cartridge features a recessed area for the label (see Figure 2-7 on page 18). The label must be applied only in the recessed label area; if it extends outside of the area it can cause loading problems in the drive.

2.3.4 Volume label format

The LTO cartridge label uses the USS-39 barcode symbols. A description and definition is available from the Automatic Identification Manufacturers (AIM) specification document *Uniform Symbol Specification (USS-39)* and *ANSI MH10.8M-1993 ANSI Bar code Specification.*

A cartridge's volume label consists of exactly 6 characters, starting from the left. Except for cleaning and diagnostic cartridges, these 6 characters are limited to the following ASCII characters:

- Upper-case A-Z (ASCII character code: 41h-5Ah)
- 0-9 (ASCII character code: 30h-39h)

The volume label must consist of exactly six, all upper-case alphabetical, all numeric, or alphanumeric characters, such as ABCGVE, 123621, or F8H5N9. It cannot consist of fewer than six characters.

A volume label format of CLN*Unn* represent a universal cleaning cartridge. A volume label of the form CLN*vnn* is used for a unique cleaning cartridge, where *v* is an alphanumeric identifier that represents the vendor of a drive-unique cleaning cartridge. (An IBM-unique cleaner cartridge uses the label format CLNInn.) This identifier is logged in the vendor information pages in the Ultrium tape drive.

A volume label of the form DG(space)*vnn* is used for diagnostic and service cartridges. The drive uses the '*v*' to determine if the drive-unique diagnostic

ROSA 03/2005 - CN - CPMI - 0044.45
Fls. Nº 4445
3690
Doc:

cartridge is loaded. The '*nn*' represents a specific cartridge and is logged in the vendor information pages in the Ultrium tape drive.

The internal and external labels on a cartridge need not match; this means that the volume label on the bar code label need not match the volume label recorded on the tape in the tape label area when it is initialized. However, it is generally preferable for them to match to avoid confusion.

You will find more detailed information in the LTO Label specification at:

`http://www.storage.ibm.com/media/`

2.3.5 Write protect switch

The write protect switch is located at the front of the cartridge to the left of the bar code label (see Figure 2-7 on page 18). The position of the write-protect switch on the tape cartridge determines whether you can write to the tape; you cannot write to the tape when the switch is pushed to the right. When the write protect switch is set to inhibit writing, a visual lock mark such as a padlock will be visible.

In most cases, backup and recovery host application software is used to achieve the most benefit from using an LTO system. It is better to rely on the host application software to write-protect your cartridges rather than manually setting the write protect switch. This allows the host software to identify a cartridge that no longer contains current data and is eligible to become a scratch cartridge. If the switch is set and the host application sets the cartridge to scratch status, the tape drive will not be able to write new data to the tape.

2.3.6 Cleaning the cartridge

Cartridges that are physically dirty on the outside of the casing can reduce the reliability of an Ultrium tape library as well as cause the loss of recorded data. If dirt appears on the cartridge, you can wipe the outside surfaces with a lint-free cloth, which may be lightly moistened with the manufacturer's recommended tape unit cleaner or equivalent.

When cleaning a tape cartridge, do not allow anything wet (including the cleaning fluid) to contact the tape inside the casing. Make sure that all cartridge surfaces are dry before the cartridge is inserted in a drive.

2.3.7 Cartridge life

The magnetic tape inside the cartridge is made of highly durable materials. However, the tape wears after repeated cycles. Eventually, such wear can cause an increase in tape errors, records of which are stored in the LTO-CM. This

1564

means that cartridge performance can be tracked and monitored, enabling predictive failure analysis and enhancing data integrity. This tracking is done automatically, and the drive issues a message when errors on the tape exceed a certain threshold.

The IBM Ultrium Data Cartridge has a usable life of 5000 load and unload cycles in a typical office computer environment.

The data recorded on the cartridge has an archive storage life of 30 years minimum with less than 5% loss in demagnetization, when the cartridge is stored at 16° C to 25° C, 20% to 50% non-condensing humidity, and wet bulb temperature of 26° C maximum.

2.3.8 Cleaning cartridge

To support customer and application requirements and expectations for cleaning, each LTO drive vendor used to provide its own cleaning cartridge specifically for its Ultrium drives. To avoid potential interoperability problems, the LTO consortium decided to introduce a universal cleaning cartridge. IBM offers only the universal cleaning cartridge.

The IBM Ultrium LTO tape drive was intentionally designed to not require cleaning but rather to be self-monitoring and self-cleaning. Therefore the IBM recommendation is not to manually clean the tape drive regularly, but rather to use the automatic cleaning function provided with the library or by your application. Each drive determines when it needs to be cleaned and alerts the library or your application.

The cleaner cartridge can be used a maximum of 50 times to prevent recontamination of drive surfaces.

2.3.9 Cartridge handling

Tape cartridges are tough packages made of inexpensive materials capable of storing tremendous amounts of data and approaching data densities of hard disks. They can survive for years in library environments where they are being gripped and poked, loaded and unloaded. But we recommend treating tape cartridges in a similar fashion to hard disk drives. Here are some suggestions to protect your data on tape cartridges.

Ensure that proper procedures are in place to cover media handling, and make sure that anyone who handles cartridges has been trained in those procedures.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1446
Fls. Nº
3690
Doc:

Media shipping and handling: procedures

Ship cartridges in their original packaging, or preferably, ship/store in jewel cases. Use only recommended shipping cases that securely hold the cartridges in their jewel cases for transportation. Turtle Cases from Perm-A-Store at www.turtlecase.com, shown in Figure 2-11, have been tested and found to be satisfactory.

Figure 2-11 Turtle case

Never ship a cartridge in a commercial shipping envelope without boxing or packaging. If shipping in cardboard or similar boxes:

- Double-box the cartridges with padding between the boxes, as shown in Figure 2-12 on page 27.
- Pack snugly so cartridges do not rattle around.
- If possible, place cartridges in polyethylene plastic wrap or bags to help seal out dust, moisture, and other contaminants.

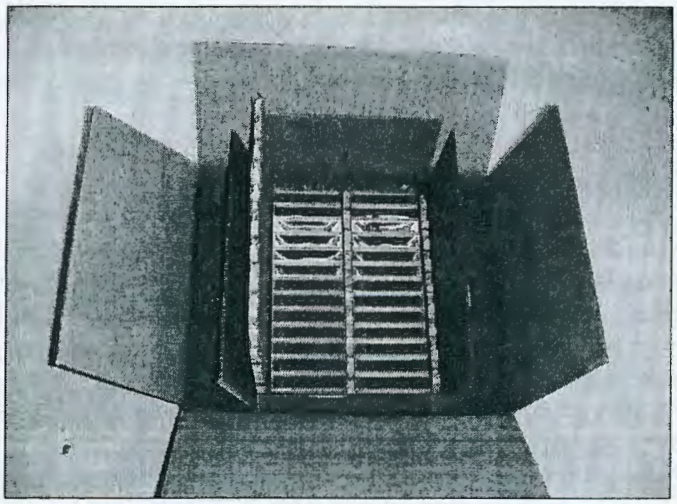


Figure 2-12 Double box

Media shipping and handling: inspecting

If you receive media, inspect it before use:

- Inspect packaging for evidence of potential rough handling.
- Inspect cartridge for damage before using/storing.
- Check leader pin for correct seating.
- When there is evidence of poor handling or shipping, ensure the cartridge leader pin (Figure 2-13) is undamaged before inserting the cartridge in a drive or library, as a bad cartridge can damage a drive.

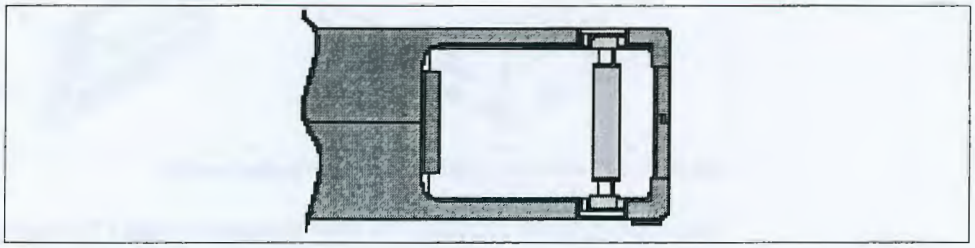


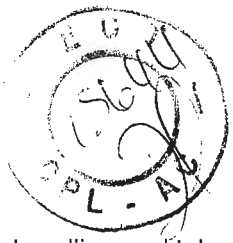
Figure 2-13 Correct leader pin placement

If the pin is loose or bent, then look for cartridge damage and use the IBM Leader Pin Re-Attachment Kit - Part Number 08L9129 to correctly seat the pin.

Summary

- Package appropriately for shipping.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1447
Doc 3690



- Inspect for damage or rough handling and take appropriate action.
- Do not put damaged media in drives or libraries; use data recovery services.
- For specific media types, check your product's Planning and Operator Guide.
- With simple care and handling you can get the most out of your tape media.

2.4 IBM LTO Ultrium common subassembly

Some elements of the Ultrium drive design are covered by the LTO format specification, such as anything related to writing the specified data format that enables tape interchange. However, there is no strict LTO definition in terms of how the drive module is constructed, so in this area, manufacturer's drives may differ from each other in performance and specification, such as data rate or quality design points. This section therefore relates specifically to the IBM LTO implementation. However, we emphasize again that the IBM LTO Ultrium cartridges are compatible with those of all other licensed manufacturers.

The IBM LTO Ultrium common subassembly drive (Figure 2-14) is a high-performance, high-capacity tape drive. The drive records data using the specified linear serpentine recording format on 1/2-inch tape housed within the LTO Ultrium cartridge. The data tracks are located using preformatted servo tracks, as outlined in 2.1.1, "Servo tracks" on page 10.

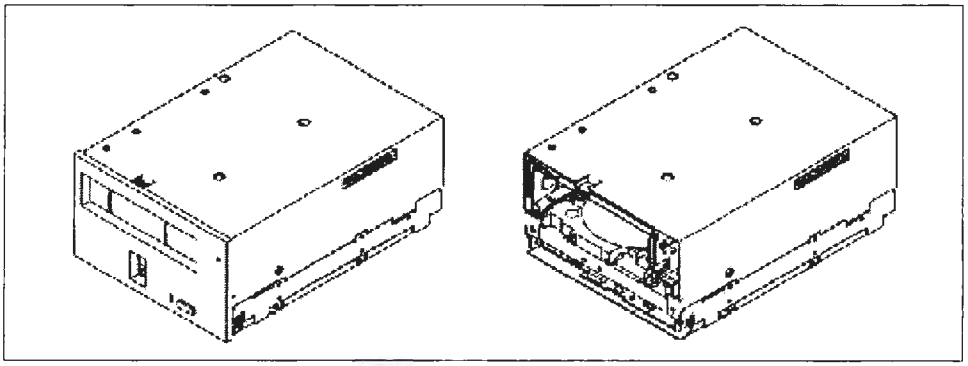


Figure 2-14 IBM LTO Ultrium common subassembly

The original basic unit was the first-generation IBM LTO series of products. The second-generation IBM LTO is a further development with a high amount of reuse, making the IBM Ultrium 2 drive very reliable. These units are a common subassembly and so do not have an IBM machine type. The subassembly is not available for end-user customers to purchase, but only as a part number used in the assembly of other IBM machine types. It does not have its own power supply but is powered by the library, frame, or casing into which it is integrated.

The IBM machine types that integrate the subassembly are described in 2.5, "The IBM LTO Ultrium family of tapes and libraries" on page 44, and in more detail in later chapters. The subassembly is sold on the OEM market to other LTO library manufacturers. The common subassembly is a single field replaceable unit (FRU): that is, if it fails the whole unit is replaced and no parts or subassemblies within the unit are replaced when the drive is maintained by a service representative.

2.4.1 Drive head

When the cartridge is inserted into the drive, a threading mechanism pulls the leader pin and attached tape (see Figure 2-9 on page 20) out of the cartridge, across the read/write head, and onto a non-removable take-up (machine) reel. The head can then read or write data from or to the tape.

The drive has a 2 x 8 element head, reading or writing data eight tracks at a time (see Figure 2-15). The head is sized to cover the width of a data recording band (approximately a quarter of the tape width; see Figure 2-4 on page 14). Unlike the IBM 3590, for example, it does not cover the whole width of the tape.

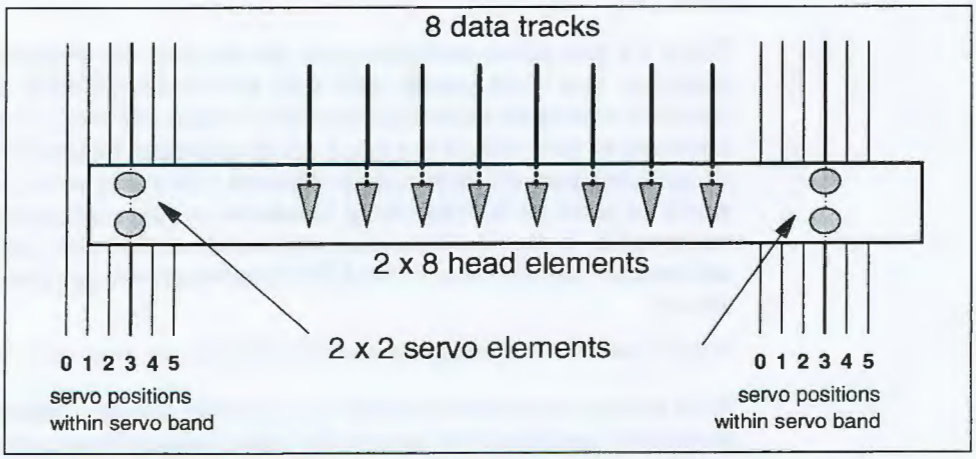


Figure 2-15 Eight-element head (one set of heads shown) and servo elements

The write elements are immediately followed by read/verify elements, so there are in fact two sets of eight head elements (eight write elements and eight read elements) to allow the tape to write in the forward and reverse directions down the length of the tape. The head switches electronically from one set to another as the tape changes direction, as in Figure 2-16 on page 30, which shows two enlarged pairs of head elements and the direction indicators. Two sets of heads (r-w and w-r) are required because the tape is written and read in both directions.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1448
Fls. Nº
Doc: 3690

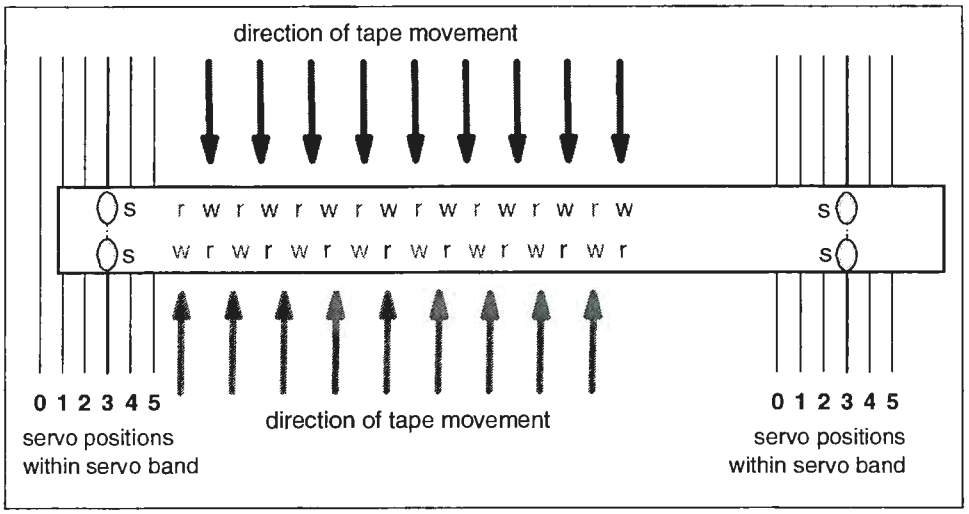


Figure 2-16 Allocation of read and write heads for forward and reverse wrap

The mechanism for writing data is explained in section 2.1.2, "Data tracks" on page 13.

There are four servo elements used, two for each set of eight read/write elements. The head actually uses both servo tracks at each edge of the data band it is writing for increased accuracy in track-following, so there are two servo elements at each end of the head. As an example, Figure 2-15 on page 29 shows a diagram of the top servo element 1 following servo position 3, which would be used for the sixth wrap (a reverse wrap) in a data band; the diagram is not to scale. If you need more information about this topic, an animated explanation can be found in the LTO Ultrium technology primers on the LTO Web site at:

`http://www.lto-technology.com/newsite/html/about_tech.html`

Note that the animation is designed to provide a basic understanding of LTO technology and does not provide the same level of detail outlined here.

2.4.2 Data compression

As describes in 2.2, "Data compression" on page 16, the implementation of the data compression may be different from vendor to vendor.

One implementation appears to only perform scheme swapping on a record basis. For example, if the compressed data stream output for a given record is larger for Scheme 1 than for Scheme 2, then the entire record is output in Scheme 2. The second implementation seems to react to data on an ongoing

basis so that if the drive perceives that the nature of the data in a record has changed from compressible to incompressible then a Scheme 2 swap is enabled and the incompressible data from there on is output in Scheme 2. This is not always advantageous because the incompressible data may again transition to compressible even before that scheme swap has occurred. Each scheme swap codeword output is 13 bits long. Therefore, to swap to a scheme and swap back costs 26 bits. The compression gain following the first scheme swap may benefit more than 26 bits over the previous scheme; if so, the swap was well-advised. If not, then the scheme swap actually increased the size of the output compressed data stream and reduced the compression rather than increase it. There is a chance of this occurring if data compressibility is inferred by having the data compression engine observe how data that has already been output from the compression engine was compressed—that is, only by viewing data in the past. The only way to adapt via scheme swapping within records, without being susceptible to inadvertent data expansion, is to use the IBM-patented scheme swapping technique. This method is preferred since it effectively looks at data ahead, rather than behind. In the IBM implementation, a scheme swap is not automatically generated unless there appears to be more compression gain within the look ahead buffer than it costs to scheme swap, and then swap back. This is advantageous as small bursts of compressible data within an otherwise incompressible file may not make it worthwhile to scheme swap. If a scheme swap is optimal, the IBM implementation puts the scheme swap out where the change in data compressibility occurs, giving maximum advantage. For more information, see:

`http://www.storage.ibm.com/hardsoft/tape/lto/prod_data/whitepaper_compression.pdf`

This paper shows how the IBM LTO-DC embodiment achieved superior data compression to another vendor's LTO drives by performing scheme swapping simultaneously with changes in the compressibility of the data, enabled by effectively looking 64 bytes ahead in the input data stream.

2.4.3 Interfaces

The IBM LTO Ultrium drive is available with a choice of interfaces, either SCSI LVD or HVD, or FC. When ordering an IBM product offering, you choose the drive interface. You cannot change the interface on the drive; if you want a different interface, you must replace the drive assembly.

Common interfaces for tape drives

Historically, SCSI connections were used for attachment of tape drives and libraries to open systems. Fibre Channel connections using SANs are becoming increasingly common.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1449
3690
Doc:

SCSI single ended

This was the most common form of SCSI signaling. Many removable drives, scanners, and almost all 50-pin SCSI devices fit into this category. Often you do not see "SE" or "single-ended" written on the documentation; if a device does not specifically say LVD, Ultra2 Wide, differential, or some similar definition, then it is probably single-ended. Typically, single-ended devices support a total bus length of 1.5 meters (5 ft) or less.

IBM high-performance SCSI tape drives (IBM 3590, IBM 3570, and LTO Ultrium drives) are all differential-attached drives, not single-ended.

SCSI differential (HVD)

HVD (often referred to as just "differential") uses differential signaling. The idea behind differential signals is that each bus signal is carried on a pair of wires. The first wire of the pair carries the same type of signal as single-ended SCSI. However, the second wire of the pair carries its logical inversion. The receiver of the signals takes the difference of the pair (hence the name), which makes it less susceptible to noise and capable of supporting greater cable lengths. HVD and single-ended SCSI are completely incompatible with each other.

In general, IBM HVD tape devices support an overall bus length of 25 m, using point-to-point or multi-drop interconnection (daisy-chaining). For each daisy-chain device you have to reduce the maximum cable length by 0.5 m.

SCSI differential (LVD)

This newer differential interface implementation, LVD uses less power than the HVD differential interface, and allows the higher speeds of Ultra-2 SCSI. LVD requires 3.3 V dc instead of 5 V dc for HVD.

LVD is sometimes referred to as Ultra-2 Wide SCSI, which is a general marketing term for 16-bit Fast-40 or 80 MB/s. Only LVD and HVD could potentially run in Ultra-2 Wide mode, and only LVSD in current commercially available products.

IBM LVD tape devices support a bus length of 25 m point-to-point, and 12 m using multi-drop interconnection (daisy-chaning). For each daisy-chain device you have to reduce the maximum cable length by 0.5 m.

The terms fast, wide, and ultra indicate characteristics that are separate from those implied by differential, single-ended, and high or low voltage. Table 2-2 on page 33 shows the SCSI terms used to describe different host and device adapters and what they imply in terms of bus width and speed.

Table 2-2 SCSI terms and characteristics

SCSI term	Bus width (bits)	Speed (MB/s)	Max. length	Max. devices
SCSI	8	5	6 m	7
Fast SCSI	8	10	3 m	7
Fast Wide SCSI	16	20	3 m	15
Ultra (Wide) SCSI HVD	16	40	25 m	15
Ultra (Wide) SCSI 2 LVD	16	80	25 m / 12 m	15
Ultra 160 SCSI LVD	16	160	25 m / 12 m	15

Note that a faster bus does not imply that an attached device will support that data rate, but that multiple devices can operate on the bus at that maximum speed. For a detailed table of SCSI terms and related specifications, refer to the SCSI Trade Association Web site at:

`http://www.scsita.org/terms/scsiterms.html`

To ensure best performance, if possible, avoid daisy-chaining.

FC-AL

The first FC-connected tape drives, such as IBM 3590 and IBM Ultrium 1, used Fibre Channel - Arbitrated Loop (FC-AL) attachment. Because IBM tape devices support public loop, those devices were seen in a SAN fabric as regular devices with a WWN, when connected to a switch supporting FC-AL login, such as Brocade and Inrange Switches and Directors.

FC switched fabric - N-Port

Newer tape devices, such as IBM Ultrium 2, use switch fabric connection (N-Port). This eliminates the need for edge loop-switches that support FC-AL login, such as the MC-Data ES1000.

Connector types

When ordering cables, pay careful attention to the type of connector on both the cable and device, so that everything will correctly plug in together. These are the major connector types.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1450
Doc: 3690

SCSI HD68

The HD68 connector is the normal 68-pin SCSI connector. All IBM LTO SCSI Drives, except the drives in the 3584, have an HD68 connector. Before June 12, 2001, all LTO tape drives in the 3584 used HD68 connectors.

Figure 2-17 HD68 connector

SCSI VHDCI

The VHDCI (Very High Density) connector is a mini-SCSI connector, about half the width of the HD68 connector. All IBM LTO drives in the 3584 have a VHDCI connector.

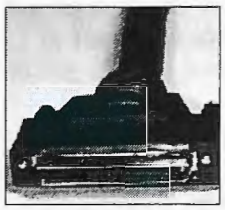


Figure 2-18 VHDCI connector

FC SC

The duplex SC connector is a low-loss, push/pull fitting connector. The two fibers each have their own part of the connector. The connector is keyed to ensure correct polarization (transmit to receive and vice-versa) when connected. Most 1 Gb SAN devices, including IBM Ultrium 1 FC drives, use SC connectors.

FC LC

Connectors that plug into SFF or SFP devices are called LC connectors. A duplex version is also used so that the transmit and receive are connected in one step. The main advantage of these LC connectors over SC connectors is that they use a smaller form factor and so manufacturers of Fibre Channel components can provide more connections in the same amount of space.

Most 2 Gb SAN devices, including IBM Ultrium 2 FC drives, use LC connectors.

Available interfaces for IBM Ultrium 1

IBM Ultrium 1 drives offer these connection types:

- Ultra2/Wide Low Voltage Differential (LVD) SCSI using VHDCI connector
- Ultra/Wide High Voltage Differential (HVD) SCSI using VHDCI connector
- FC-AL, 1 Gbps using SC connector

Available interfaces for IBM Ultrium 2

IBM Ultrium 2 drives offer these connection types:

- Ultra 160 Low Voltage Differential (LVD) SCSI using VHDCI connector
- Ultra/Wide High Voltage Differential (HVD) SCSI using VHDCI connector
- Switched fabric 2 Gbps using LC connector

2.4.4 Performance

IBM LTO drives provide high performance and will continue to improve with each new generation of products. If you run applications that are highly dependent on tape-processing speed, you can exploit the significant performance provided by the Ultrium tape drives.

IBM Ultrium 1

The IBM LTO Ultrium 1 tape drive has these performance characteristics:

- 15 MB/s native sustained data transfer rate
- 30 MB/s sustained data transfer rate at 2:1 compression
- 60 MB/s maximum sustained data rate (at maximum compression)
- 100 MB/s burst data transfer rate for Fibre Channel
- 80 MB/s burst data transfer rate for Ultra-2 SCSI LVD drives
- 40 MB/s burst data transfer rate for Ultra SCSI HVD drives
- 20 s nominal load-to-ready time
- 18 s nominal unload time
- 73 s average search time to first byte of data
- 110 s maximum rewind Time
- 4 m/s read/write speed
- 6 m/s search/rewind speed
- 32 MB buffer

IBM LTO Ultrium drives provide efficient tape operations and relief to users who have difficulty completing tape activities in the time available. If you have limited system backup windows, or if you have large amounts of disk data to back up, Ultrium tape drives are ideal.

By using the built-in data-compression capability of the Ultrium drive, you can potentially achieve greater data rates than the uncompressed data rate.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1451
Doc 3690

However, the actual throughput is a function of many components, such as the host system processor, disk data rate, block size, data compression ratio, SCSI bus capabilities, and system or application software. Installing multiple tape drives in general (or more than two in the case of IBM LTO) on a single SCSI bus may adversely affect data transfer rates.

IBM Ultrium 2

The IBM LTO Ultrium 2 drives provide more than twice the performance over IBM Ultrium 1 with sustained data rates of 35 MB/s native and 70 MB/s with 2:1 compression. IBM Ultrium 2 has faster load and unload time, faster data access time, faster rewind time, and faster cartridge fill time compared with IBM Ultrium 1.

The IBM LTO Ultrium 2 tape drive has these performance characteristics:

- 35 MB/s native sustained data transfer rate
- 70 MB/s sustained data transfer rate at 2:1 compression
- 110 MB/s maximum sustained data rate (at maximum compression)
- 200 MB/s burst data transfer rate for Fibre Channel
- 160 MB/s burst data transfer rate for Ultra 160 SCSI LVD drives
- 40 MB/s burst data transfer rate for Ultra SCSI HVD drives
- 15s nominal load-to-ready time
- 15 s nominal unload time
- 49s average search time to first byte of data
- 80 s maximum rewind Time
- 6.2m/s read/write speed
- 8m/s search/rewind speed
- 64 MB buffer

2.4.5 Partial Response Maximum Likelihood (PRML)

The IBM patented linear tape implementation of a Partial Response Maximum Likelihood (PRML) channel technology increases linear densities up to 33% and consequently data throughput. The key to PRML's space-saving capability is that on a read-back operation, the magnetic flux transitions are sampled and the sampling feeds logic algorithms that reconstruct the user's data stream, rather than using the flux transitions themselves. The previous method of data encoding was RLL (Run Length Limited) encoding, also patented by IBM for use in earlier tape drives. Figure 2-19 on page 37 compares both methods.

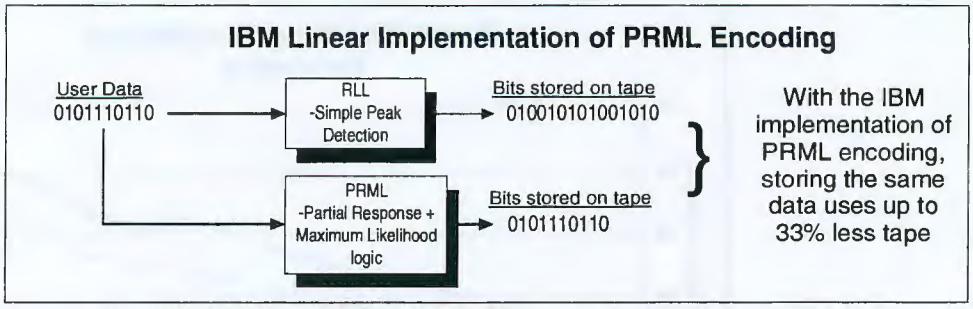


Figure 2-19 IBM linear implementation of PRML encoding

2.4.6 IBM Ultrium 2: additional improvements

On top of the improved performance and capacity, IBM Ultrium 2 provides additional benefits.

Dynamic speed matching

The Ultrium 2 Tape Drive performs dynamic speed matching to adjust the drive's native data rate as closely as possible to the net host data rate (after data compressibility has been factored out). This provides the dual benefit of reducing the number of backhitch repositions and improving throughput performance.

The drive can run in five different speeds: 4/8, 5/8, 6/8, 7/8, and full speed. This results in data transfer rates of 17.5 MB/sec, 21.9 MB/sec, 26.3 MB/sec, 30.6 MB/sec, and 35 MB/sec.

At net host data rates of 17-32 MB/sec, the average throughput performance benefit is 13% when compared with speed matching disabled. At speeds below 17 MB/sec, the drive's 64MB internal buffer masks the performance degradation of repositions. At speeds greater than 32 MB/sec, the drive operates at its fastest possible speed (same speed as speed matching disabled). At net host data rates of 1-32 MB/sec, the average reposition reduction benefit is 68% when compared to speed matching disabled.

Figure 2-20 on page 38 shows the throughput improvement in MB/sec with speed matching enabled relative to speed matching disabled. The statistics show that at each host data rate from 17-32 MB/sec, speed matching enabled improves throughput. Data points from 1-16 and from 33-40 were removed for clarity. At those data points, there is no difference between speed matching enabled vs. disabled as explained in the previous paragraph.

REQS nº 03/2005 - CN - CFMI - CORREIOS
Fls. Nº 1452
Doc: 3690

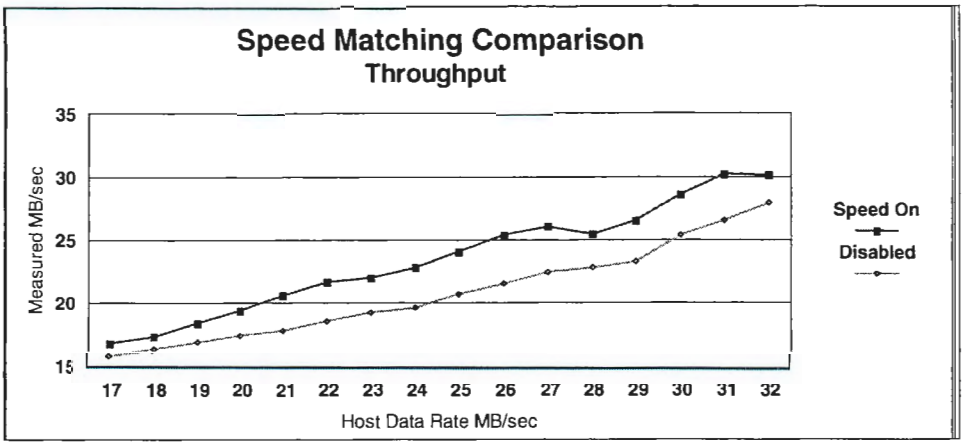


Figure 2-20 Speed matching comparison: MB/sec

If an LTO 1 cartridge is used in an LTO 2 drive, then the LTO 2 drive operates at 5.34 m/sec with no speed matching. While running at 5.34 m/sec, the LTO 2 drive will read and write at 20 MB/sec because of the smaller linear density. There is no need for speed matching when using LTO 1 media, because at the buffer size of 64 MB, the backhitch is transparent. This means that after a start/stop of the drive, the repositioning time is less than the time to fill up the buffer.

Power management

The Ultrium 2 Tape Drive power management function controls the drive electronics to be either completely turned off or to be in a low-power mode. These power modes occur only when the circuit functions are not needed for drive operation.

Channel calibration

The Ultrium 2 tape drive channel calibration feature allows for customization of each read/write data channel for optimum performance. The customization enables compensation for variations in the recording channel transfer function, media characteristics, and read/write head characteristics.

Separate writing of multiple filemarks

Separate writing of multiple filemarks means that any write command of two or more filemarks will cause a separate data set to be written containing all filemarks after the first. This feature has two advantages. First, it improves performance if a subsequent append overwrites somewhere after the first filemark. Second, writing multiple filemarks typically indicates a point where an append operation might occur after the first of these filemarks. This change

prevents having to rewrite datasets containing customer data and the first filemark if such an append occurs.

2.4.7 IBM Ultrium 1 and 2 compatibility

IBM Ultrium 2 tape drives (both standalone and in IBM Ultrium libraries) support both Ultrium 1 and Ultrium 2 cartridges. An Ultrium 1 cartridge in an Ultrium 2 drive will be written at the same 100 GB native capacity, but with improved performance (20 MB/s). Ultrium 1 drives cannot read or write an Ultrium 2 cartridge. If you put an Ultrium 2 cartridge in an Ultrium 1 drive, then you will get an "Unsupported Cartridge Format" failure. Figure 2-21 shows the compatibility.

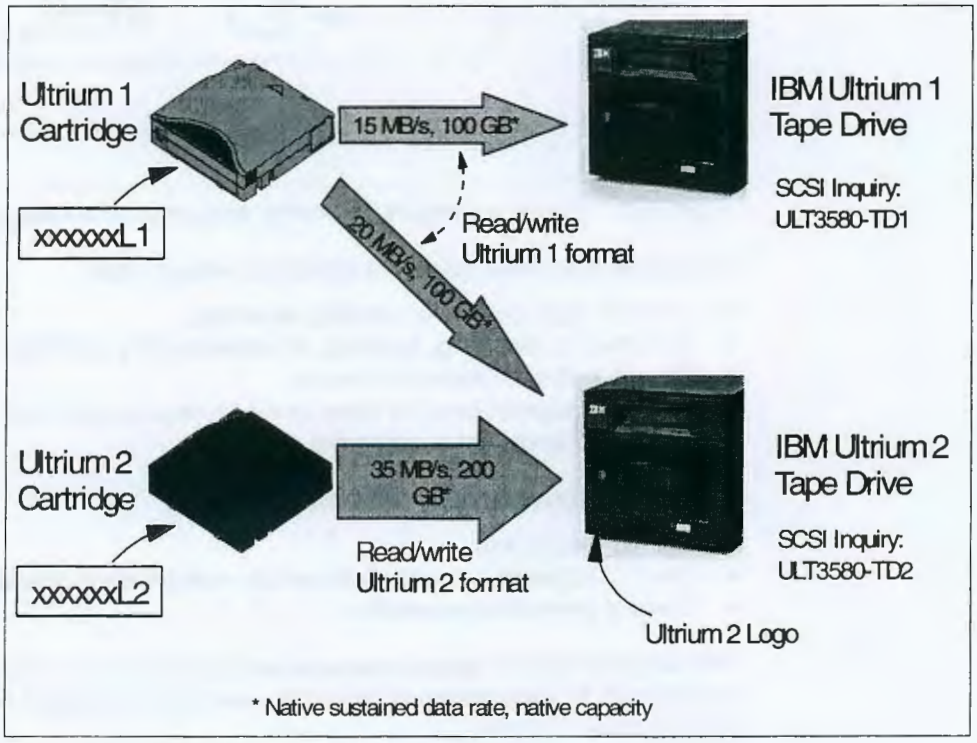


Figure 2-21 IBM Ultrium 1 and 2 compatibility

2.4.8 Operating the Ultrium drive

The IBM subassembly itself has a simple status LED indicator, an unload push button, and a single-character display (see Figure 2-22 on page 40).

POS nº 02.2005 - CN - CPMI - CORREIOS
1453
Fls. Nº
Doc 3690

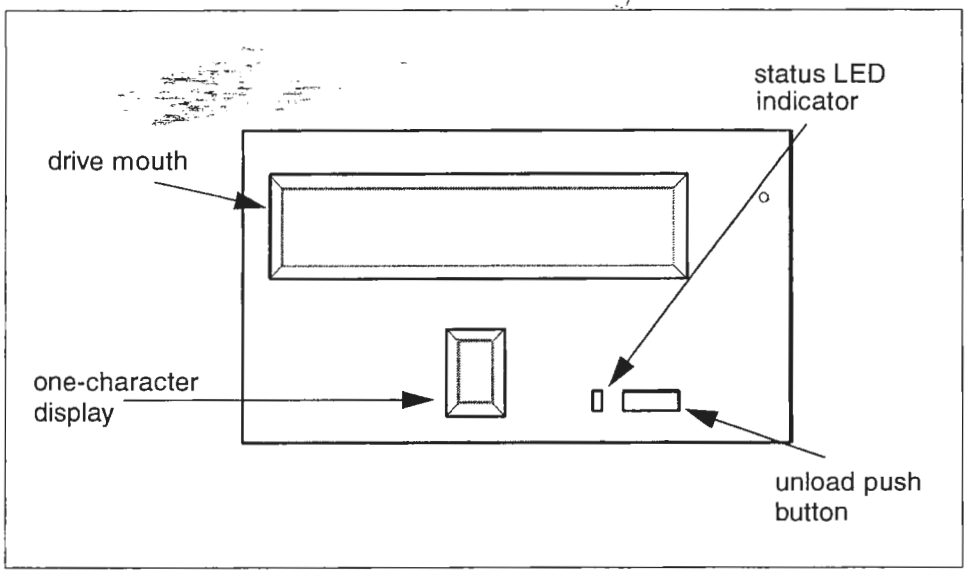


Figure 2-22 Front of subassembly showing operator panel indicators

The status LED uses color and lighting to indicate that:

- The tape is in motion for reading or writing.
- The drive is rewinding, locating, or unloading the cartridge.
- The drive is in maintenance mode.
- A failure occurred and the drive or media requires service.
- A microcode update is occurring.

The unload push button enables the operator to:

- Unload a cartridge
- Enter maintenance mode and execute maintenance operations
- Force a drive dump operation

The single-character display indicates errors and communicates messages, such as requests for cleaner tapes. It is also used by the operator for diagnostic and maintenance functions.

2.4.9 Reliability

The IBM LTO Ultrium tape format differs from earlier IBM products. Reliability and availability features include:

- Data integrity

  The drive performs a read after write, for verification. Incorrectly written data, such as the result of a tape defect, is automatically rewritten by the drive in a new location. Data rewritten as the result of media defects is not counted against the drive error performance.

  The drive will never record incorrect data to the tape media without posting an error condition.

- Power loss

  No recorded data is lost as a result of normal or abnormal power loss while the drive is reading or writing data. If power is lost while writing data, only the data block currently being written may be in error. Any previously written data will not be destroyed.

- Error correction

  Data integrity features include two levels of error correction that can provide recovery from longitudinal media scratches.

- Integrated head cleaner

  The head of the drive must be kept clean to prevent errors caused by contamination. During the load process, a brush integrated into the drive mechanism cleans the head before it is used with the tape. This keeps the head and media free of debris on a continuing basis and is expected to lead to less requirement for drive-cleaning operations.

- Surface control guiding

  IBM's patented Surface Control Guiding Mechanism guides the tape along the tape path using the surface of the tape rather than the edges to control tape motion. Through grooved rollers (see Figure 2-23 on page 42), an air cushion builds between the tape and the rollers that keep it in the right position. This results in less tape damage (especially to the edges of the tape) and less debris from damaged edges that can accumulate in the head area, and helps minimize the chance of physical damage to the tape media.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1454
Fls.: Nº
Doc: 3690

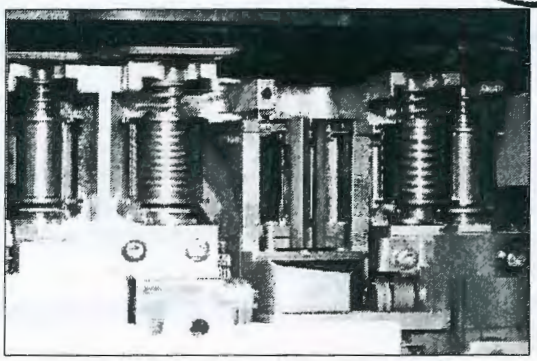


Figure 2-23 Surface control guiding

- Flat lap head

  The flat head improves contact between the read and write recording elements and the tape, giving higher quality recording and readback of data.

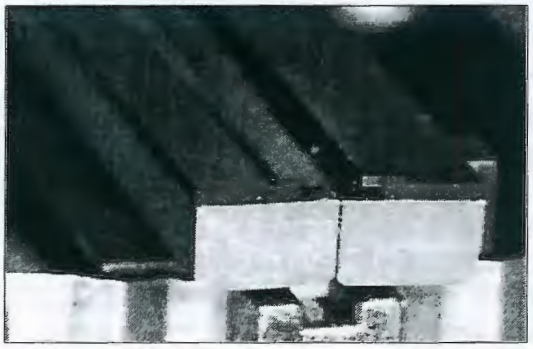


Figure 2-24 Flat lap head

Surface control guiding and the flat lap head are designed to help minimize debris generated as the tape moves through its path, resulting in increased reliability in reading and writing data. This also potentially increases the life expectancy of the media by not using the edges of the tape to guide it over the read/write head. Historically, this also was a major source of debris on the tape path.

- Statistical Analysis and Reporting System

  Statistical Analysis and Reporting System (SARS) is another IBM exclusive. Only IBM LTO drives provide this level of preventive diagnostic reporting. The Ultrium drive uses this reporting system to assist in isolating failures between media and hardware. SARS uses the cartridge performance history saved in the CM module and the drive performance history kept in the drive flash

EEPROM to determine the most likely cause of failure. It then can cause the drive to request a cleaner tape, to mark the media as degraded, and to indicate that the hardware has degraded. SARS reports the results of its analysis in the form of Tape Alert if needed (see Figure 2-25).

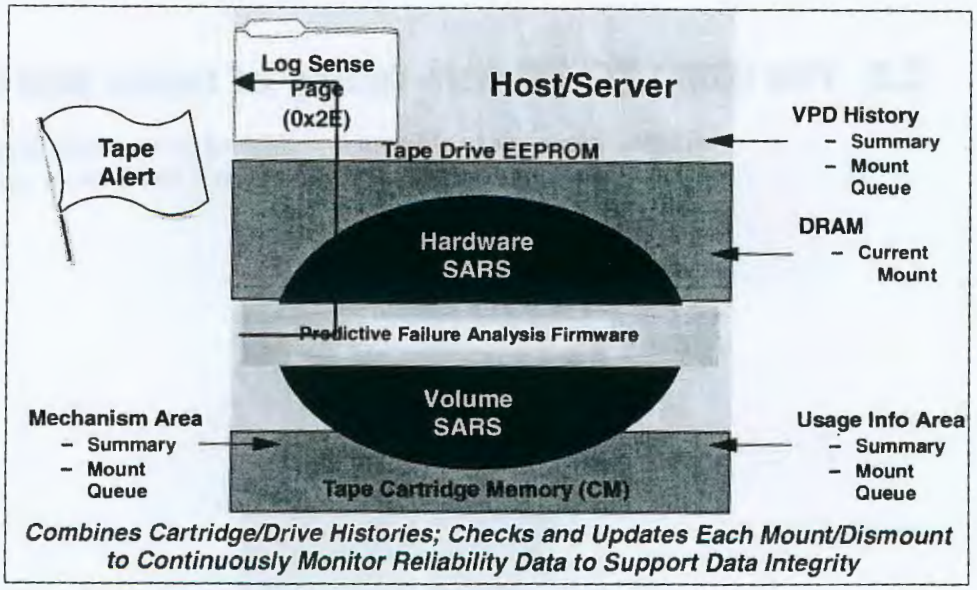


Figure 2-25 Statistical Analysis and Reporting System

2.4.10 Cleaning the drive

In addition to the integrated head-cleaning mechanism, IBM recommends that the drive be cleaned regularly, with automatic cleaning enabled where supported in the libraries. Regular cleaning avoids drive shutdowns because of improper maintenance or contaminants that cause the drive to fail.

In the unusual event that the drive head becomes clogged, it *may* be necessary to use the specially labeled IBM LTO Ultrium cleaning cartridge supplied with each Ultrium tape drive product. The cleaning cartridge is good for 50 cleaning operations. If cleaning proves necessary, the LTO-CM memory in a cleaning cartridge is used to track the number of times that the cartridge has been used. After the cartridge has been used 50 times, the drive will mark the cleaning cartridge as expired. This also protects you from accidentally reinserting a cleaning cartridge that has been used 50 times.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1455
Doc: 3690

Note: The use of cleaning cartridges is not necessary (and is discouraged) for normal operation of Ultrium tape drives. See *3580 Ultrium Tape Drive Setup, Operator, and Service Guide*, GA32-0415, for information about drive cleaning.

2.5 The IBM LTO Ultrium family of tapes and libraries

The IBM Ultrium family of tapes and libraries (pictured in Figure 2-26) comprises five different product offerings, ranging from a stand-alone unit to a highly scalable automated library.

Figure 2-26 The IBM Ultrium family of tapes and libraries

They are all based on a common tape drive subassembly packaged in different robotic and stand-alone environments.

- The *IBM TotalStorage Ultrium Tape Drive 3580* is a stand-alone desktop single-drive unit without autoloader. Tapes are mounted manually one at a time.
- The *IBM TotalStorage Ultrium Tape Autoloader 3581* is also a single-drive unit, but it has a seven-cartridge autoloader within the device. It is a stand-alone desktop unit; however, optional additional hardware is available for installation in a standard 19-inch rack.
- The *IBM TotalStorage Ultrium Tape Library 3582* is a small robotic library, accommodating one to two drives and providing space for up to 23 Ultrium cartridges. The IBM 3582 may be stand-alone or, with an optional feature, housed in a rack.
- The *IBM TotalStorage Ultrium Scalable Tape Library 3583* is a small robotic library, accommodating from one to six drives and providing space for up to 72 Ultrium cartridges. The IBM 3583 may be standalone or, with an optional feature, housed in a rack.
- The *IBM TotalStorage UltraScalable Tape Library 3584* is a larger modular library with the potential to house a maximum of 192 tape drives in as many as 16 frames. There is a trade-off between cartridge capacity and installed drives, so that a fully-configured library with 192 drives and a 10-cartridge I/O station has a cartridge capacity of 6167; with a minimal drive configuration the cartridge capacity can reach a maximum of 6881.

Storage and tape management for the IBM LTO Ultrium family is provided by software such as IBM Tivoli Storage Manager and other similar software offerings.

These products, while all part of the same family, are distinct offerings. The drive and cartridge technology and formats are the same, and the cartridges are interchangeable between the libraries, as dictated by the LTO format standards. However, the machine types (for example, 3583 and 3584) are not upgradeable from one to another, nor can the Ultrium drives be exchanged between different libraries. Thus, if you purchase an IBM 3583 with six drives and later on install an IBM 3584, you cannot transfer the Ultrium drives from the 3583 to the 3584.

Detailed descriptions of these products can be found in Chapter 4, "IBM TotalStorage Ultrium Tape Drive 3580" on page 79, through Chapter 8, "IBM TotalStorage UltraScalable Tape Library 3584" on page 159.

The IBM LTO family of products is sold directly through IBM and its Business Partners.

CPMI - CORREIOS
Fls. Nº 1456
Doc 3690

2.6 Multi-path architecture

This patented multi-path architecture was introduced with the IBM Magstar MP 3575 library. It provides a way to share a tape library between a number of servers without the need to implement application software to control and serialize tape drives and media. It is also implemented in the IBM 3582, 3583, and 3584 libraries.

Multi-path architecture is an IBM unique feature. The IBM 3582, 3583, and 3584 LTO libraries feature the second generation of the architecture introduced with the Magstar MP 3575 library. It uses the SCSI-3 Move Media command set that is featured in midrange and open libraries. The key benefit is that multi-path architecture removes the need for a dedicated server plus middleware to control the use of a library by many different hosts utilizing different operating systems, as each drive has its own path to the control unit.

Conventional tape libraries use a dedicated host port to communicate to the library, such as to send mount request commands. IBM LTO tape libraries use the same path to communicate with both the drives and the library controller, as shown in Figure 2-27. This is not one dedicated path, but it may be any path to any tape drive.

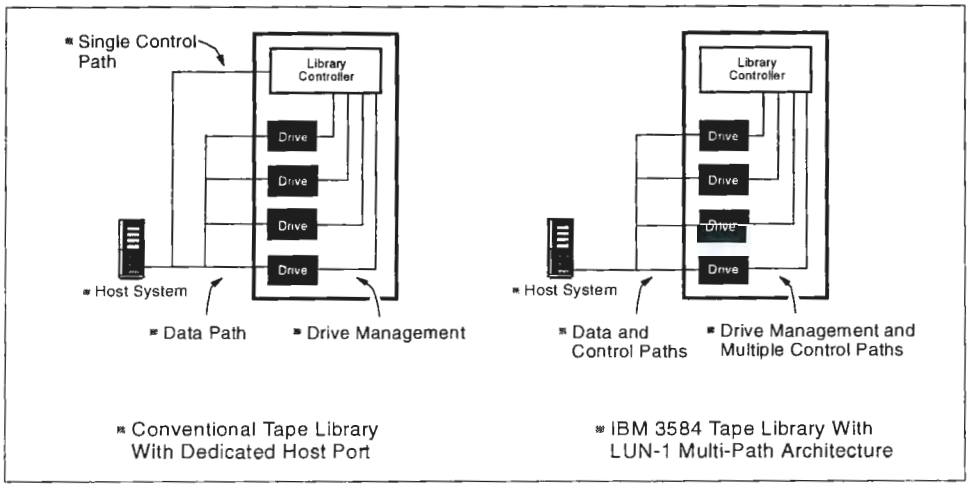


Figure 2-27 Conventional tape library vs. multi-path architecture

For conventional tape libraries, the control path is a single point of failure. In contrast, the IBM LTO tape libraries offer as many control paths as there are drives installed in the library, so in the event of individual control path failure you can communicate with your library over different, redundant control paths. As shown in Figure 2-28 on page 47, if one path to a drive is broken because of a

defective switch port, cable, or HBA, communication to the library controller can still occur using one of the other available paths. In conjunction with automatic Control Path Failover, this constitutes a unique high-availability option.

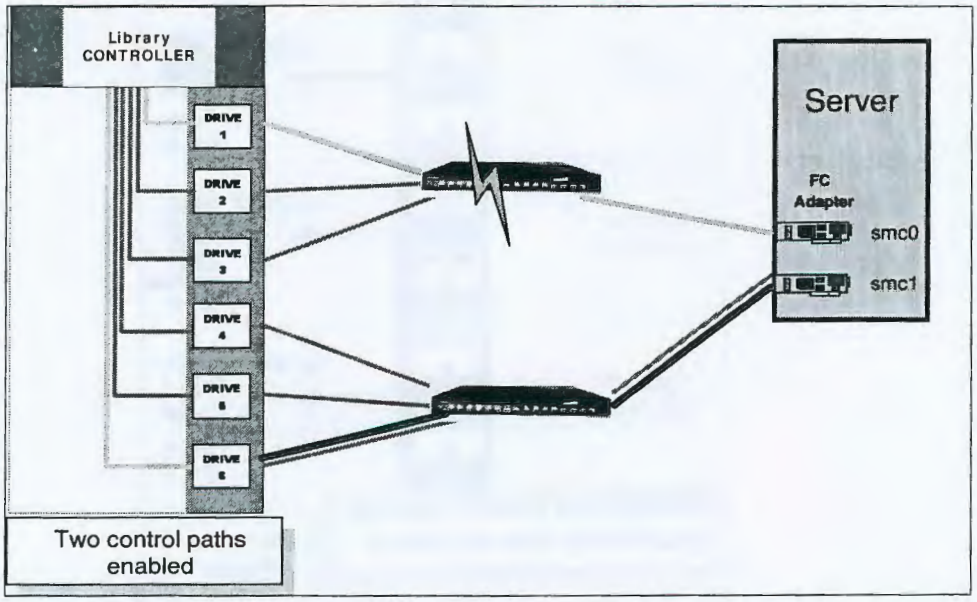


Figure 2-28 Redundant control paths to the library controller

As well as the redundant control path, multi-path architecture offers the additional benefit of built-in partitioning. With the partitioning feature of the IBM LTO libraries, you can divide the physical library into several smaller logical libraries, which are independent from each other. The maximum number of logical libraries varies by model type. A logical library must contain at least one tape drive and can comprise more than one tape drive sharing the same cartridge cells.

With this partitioning option, the library can be shared between multiple heterogeneous hosts. Each logical library has its own drives, cartridges, and control paths. Because of barriers between the logical libraries, cartridges cannot be moved from one logical library to another. Figure 2-29 on page 48 shows three logical libraries with two drives each and some cartridge storage slots dedicated to each of the heterogeneous servers.

RQS nº 03/2005 - CN -
CPMI---CORREIOS
Fls. Nº 1457
Doc: 3690

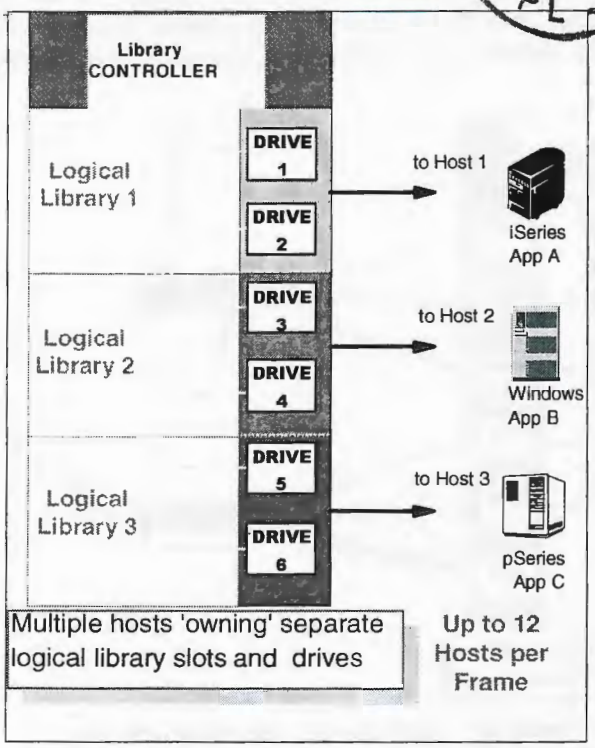


Figure 2-29 IBM LTO tape library partitioned into three logical libraries

3

Tape storage market direction

Tape systems traditionally have been associated with the mainframe computer market, because they have represented an essential element in mainframe systems architectures since the early 1950s as a cost-effective way to store large amounts of data. The mid-range and client/server computer market has, in contrast, made very limited use of tape technology until quite recently.

Over the past few years, however, the growth in the demand for data storage and reliable backup and archiving solutions has greatly increased the need to provide manageable and cost-effective tape library products. The value of using tape for backup purposes hasonly gradually become obvious and important in these environments.

In this chapter, we will review the technologies, formats, and standards that you will see for tape products in today's market. We discuss a number of products from non-IBM vendors and, although we have reviewed the material carefully, we would remind you that the vendors of those products are the definitive source of information.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1458
3690
Doc:

3.1 Current tape products and technologies

Two basic tape technologies have been utilized. Until the middle of the 1980s, all computer tape systems utilized linear recording technology, a technology that uses a stationary head writing data in a longitudinal way (see Figure 3-3 on page 54 for an example of longitudinal technology).

In the middle of the 1980s, helical tape technology (which had been developed for video applications) became available for computer data storage, a technology that uses heads rotating on a drum and writing data in an angle. Helical tape systems found natural applications in backing up magnetic disk systems where their cost advantages substantially outweighed their operational disadvantages (see Figure 3-4 on page 55 for an example of helical-scan technology).

3.1.1 Helical versus longitudinal

The first computer tape systems used linear recording technology. This technology provides excellent data integrity, rapid access to data records, and reasonable storage density.

The first implementation of linear recording technology used magnetic tapes on open reels. Later, the tape was protected inside cartridges, using one or two reels. Linear technology drives write each data track on the entire length of the tape. Data is first written onto a track along the entire length of the tape, and when the end is reached, the heads are repositioned to record a new track again, along the entire length of the tape, now travelling in the opposite direction. This continues back and forth until the tape is full. On linear drives, the tape is guided around a static head.

On helical scan systems, by contrast, the tape is wrapped around a rotating drum containing read/write heads. Due to the more complicated path, mechanical stress is placed on the tape. When contrasted with linear tape systems, helical tape systems have higher density (and, therefore, lower media cost), but lower data transfer rates (due to the smaller number of active read/write heads), less effective access to random data records, increased maintenance requirements, and reduced data integrity.

Both linear and helical tape systems have advanced substantially over the past decade. Linear systems have improved significantly in the areas of storage density (and, therefore, cost), and operational convenience (with a variety of removable cartridge systems such as 3590, QIC, DLT, and now LTO replacing reel-to-reel systems). Helical systems have improved in the areas of transfer rate and data integrity with the implementation of both channel and error correction coding technologies.

Over the past few years, one of the most significant advances in tape technology for computer applications has been the maturation of serpentine linear recording systems which, for the first time, has permitted linear recording systems to provide recording density that is comparable with that of helical systems. The first commercially successful serpentine linear tape system for professional applications was DLT. Another important improvement is the use of servo tracks, first introduced by IBM on the Magstar 3590 tape. Servo tracks on the tape cartridge are recorded at the time of manufacture. These tracks enable the tape drive to position the read/write head accurately with respect to the media while the tape is in motion.

Most linear media is manufactured using metal particle (MP) technology. As with most tape products, metal particle media comprises several layers: a substrate that provides the base for other layers, the magnetic layer where data is stored, and a back coat that controls the media's frictional characteristics.

The most advanced implementations of 8 mm format (Mammoth and AIT) use AME (Advanced Metal Evaporative) media. The AME magnetic layer is 100% cobalt and is a much thinner, pure magnetic layer that doesn't contain any binders or lubricants. These qualities give AME tapes greater potential data density so that more information can be stored on less tape surface.

Future generations of linear tape media (including LTO) will use the same AME magnetic layer technology, offering increased data densities.

We felt that the fundamental difference between linear recording and helical scan technologies is so important that it would be worthwhile to summarize all of the available current technologies (see Table 3-1).

Table 3-1 Tape technology overview

Name	Recording technology	Media width	Type
1/2-inch reels	linear	1/2 inch	single hub
QIC	linear	1/4 in and 8 mm	dual hub
DAT/4 mm	helical-scan	4 mm	dual hub
DDS	helical-scan	all 4 mm	dual hub
8 mm	helical-scan	8 mm	dual hub
Mammoth	helical-scan	8 mm	dual hub
AIT	helical-scan	8 mm	dual hub
Ecrix VXA	helical-scan	8 mm	dual hub

RQS nº 03/2005 - CN - CPMI - CORREIOS
1459
Fls. Nº
3690
Doc:

Name	Recording technology	Media width	Type
DLT	linear	1/2 inch	single hub
IBM 3480/90	linear	1/2 inch	single hub
IBM Magstar MP 3570	linear	8 mm	dual hub
IBM Magstar 3590	linear	1/2 inch	single hub
STK 9840	linear	1/2 inch	dual hub
STK 9940	linear	1/2 inch	dual hub
LTO Ultrium	linear	1/2 inch	single hub

3.1.2 Tape reels (1/2-inch)

The first data backup device (and the ancestor of magnetic tape devices with a 1/2-inch-wide tape format) used magnetic tape reels, shown in Figure 3-1. Reel tapes have been around for many years. They can support densities from 800 bpi to 6250 bpi (bits per inch) and were manufactured and sold in many different lengths and brands. The most common densities used were 1600 and 6250 bpi, but most of these devices have been replaced today.

Figure 3-1 Tape reels, 1/2-inch

3.1.3 QIC

The quarter-inch-tape cartridge (QIC) was first introduced in 1972 by the 3M company as a means to store data from telecommunications and data acquisition applications. As time passed, the comparatively inexpensive QIC drive became an accepted data storage system, especially for stand-alone PCs.

QIC cartridges (shown in Figure 3-2 on page 53) look much like audio tape cassettes with two reels inside, one with tape and the other for take-up. The reels are driven by a belt built into the cartridge. A metal rod, known as a capstan, projects from the drive motor and pinches the tape against a rubber drive wheel.

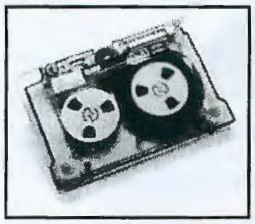


Figure 3-2 QIC cartridge

The QIC format employs a linear (or longitudinal) recording technique in which data is written to parallel tracks that run along the length of the tape. The number of tracks is the principle determinant of capacity. The cartridges come in two varieties, DC600 cartridge and DC2000 mini cartridge, the latter being the more popular. The encoding method used is either MFM (Modified Frequency Modulation) or RLL (Run Length Limited), and is similar to the way a hard drive encodes data.

When a backup is started, directory information from the file allocation table is loaded into a memory buffer in the system's RAM, along with the appropriate files. Both sets of data are sent to the tape drive controller, each file being prefaced by a header containing the directory information. If the controller has built-in error correction, an error correction code (ECC) is appended to the data in the controller. Otherwise, the software adds the code before sending the data to the controller.

The controller contains its own buffer. Once the backup data containing the ECC is in this buffer, the backup software is free to load more data into system memory. The drive's controller then sends the data as required to the tape drive mechanism.

QIC uses a linear read/write head similar to those found in domestic cassette recorders (Figure 3-3 on page 54). The head contains a single write head flanked on either side by a read head. This allows the tape drive to verify data just written when the tape is running in either direction. If the data just written is verified by the read head, the buffer is flushed out and new data is acquired from the system memory.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1460
Doc. 3690

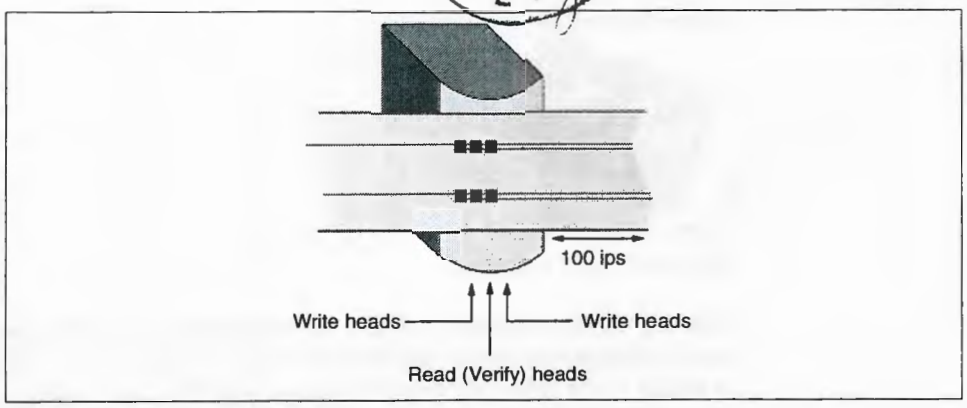


Figure 3-3 QIC head diagram

QIC standards

As the QIC standards of the time failed to keep up with the storage media explosion of the mid-1990s, the QIC cartridge underwent an evolution that increased capacities by both lengthening and widening the tape. The Sony-inspired move to a wider format tape was a noteworthy development.

One of the drawbacks with QIC is incompatibility. The format has suffered from an overabundance of standards over the years—there are more than 120 currently—and not all QIC drives are compatible with all standards.

Tandberg Data remains the only drive manufacturer in this segment with its Scalable Linear Recording (SLR) technology. Their most recent drive, the SLR100, provides 50 GB (native) and 100 GB (with 2:1 compression) capacity on a single data cartridge. The maximum data transfer rates are 5 MB/s uncompressed and 10 MB/s (with 2:1 compression).

3.1.4 Digital Data Standard (4 mm)

The Digital Audio Tape (DAT) standard was created in 1987 and, as its name implies, was originally conceived as a CD-quality audio format offering three hours of digital sound on a single tape. The Digital Data Standard (DDS) is based on DAT and uses a similar technology. The cartridge design is common, but different tape formulations have been developed. In 1988, Sony and HP defined the DDS standard, transforming the format into one that could be used for digital data storage.

DAT technology is a 4 mm tape that uses helical scan recording technology. This is the same type of recording as that used in videocassette recorders and is inherently slower than the linear type. The tape in a helical scan system is pulled

from a two-reel cartridge and wrapped around a cylindrical drum containing two read heads and two write heads, arranged alternately. The read heads verify the data written by the write heads. The cylinder head is tilted slightly in relation to the tape and spins at 2,000 revolutions per minute. The tape moves in the opposite direction to the cylindrical spin, at less than one inch per second, but because it is recording more than one line at a time it has an effective speed of 150 inches per second (refer to Figure 3-4).

Short diagonal tracks, about eight times longer than the width are written across the width of the tape. These each contain about 128KB of data and an error correction code.

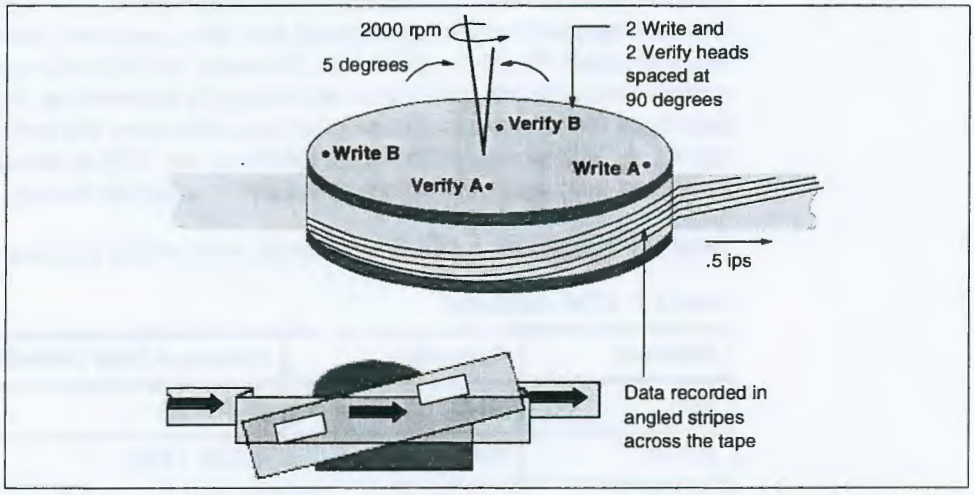


Figure 3-4 Helical-scan recording diagram

A read head verifies the data. If errors are present the data is rewritten; otherwise the controller buffer is flushed ready for the next segment. The second write head writes data at a 40-degree angle to the first one.

Even though the first and second writes overlap, they are magnetically encoded with different polarities so they are only read by the correct read head. The "criss-cross" pattern packs more data onto the tape, enabling helical scan systems to achieve very high data densities. A directory of files is stored in a partition at the front of the tape.

Just as with linear recording, the performance would be greatly improved if additional read/write heads were added, but this is difficult with helical scan devices, because of the design of the rotating head. The fact that the heads may only be added in pairs makes it difficult to fit the wiring inside a single cylinder, and this limits the potential performance of helical scan devices. Because of the

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1461
Doc: 3690

wide wrap angle of the tape and the consequent degree of physical contact, both the head and the media are prone to wear and tear.

When restoring from the backup, the backup software first reads the entire directory of the tape's contents. It then winds the tape to the appropriate spot and reads the contents into the controller's buffer. The controller uses the CRC code to make sure the information is correct. If errors are detected, the ECC can be used to fix them. Once the data has been verified as correct, the buffer contents are passed to system memory.

DDS-3 uses the same helical scanning head but adds a technology commonly used for hard disk drives, called PRML (Partial Response, Maximum Likelihood), which is used to weed out the data from electronic noise. The latest DDS-4 format, proposed by Hewlett-Packard and Sony, was endorsed by the DDS Manufacturers Group in April 1998. The extra 16 GB compressed capacity realized in this fourth-generation technology is achieved by reducing the track pitch from 9.1 microns to 6.8 microns and increasing the length of the media to 150 m. As with previous DDS specifications, the DDS-4 standard provides backward read and write compatibility with the earlier formats.

Table 3-2 shows current DDS standards, all of which are backward-compatible.

Table 3-2 DDS standards

Standard	Capacity	Maximum Data Transmission Rate
DDS	2 GB	0.55 MB/s
DDS-1	2/4 GB	0.55/1.1 MB/s
DDS-2	4/8 GB	0.55/1.1 MB/s
DDS-3	12/24 GB	1.1/2.2 MB/s
DDS-4	20/40 GB	2.4/4.8 MB/s

3.1.5 The 8 mm format

Designed for the video industry, 8 mm tape technology was created to transfer high-quality color images to tape for storage and retrieval and now has been adopted by the computer industry. Similar to DAT, but with greater capacities, 8 mm drives are also based on the helical scan technology. A drawback to the helical scan system is the complicated tape path. Because the tape must be pulled from a cartridge and wrapped tightly round the spinning read/write cylinder (Figure 3-5 on page 57), a great deal of stress is placed on the tape.

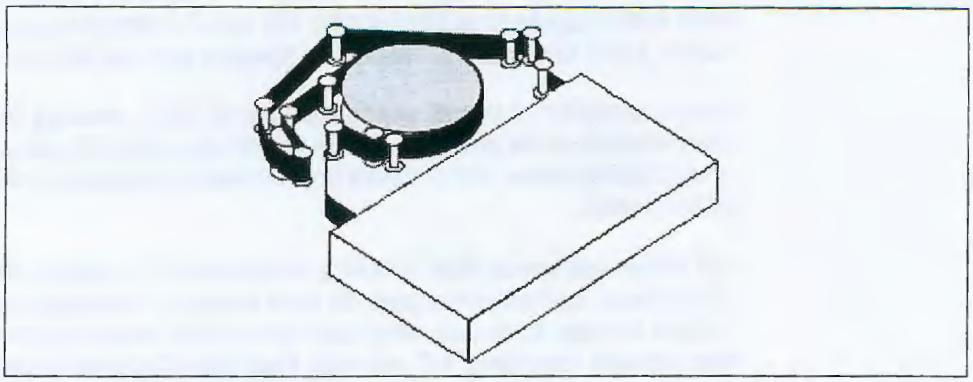


Figure 3-5 An 8 mm tape path

There are two major protocols that use different compression algorithms and drive technologies, but the basic function is the same. Exabyte Corporation sponsors standard 8 mm and Mammoth formats, while Seagate and Sony represent a new 8 mm technology known as Advanced Intelligent Tape (AIT).

Mammoth tape format

This is a SCSI-based 8 mm tape technology, designed for open system applications. It is a proprietary implementation of the 8 mm standard format available since 1987 and uses Advanced Metal Evaporative (AME) media. This media has a coating over the recording surface that seals and protects the recording surface.

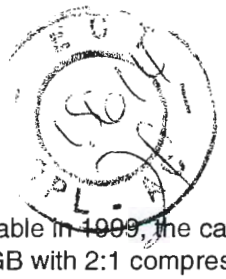
The Exabyte Mammoth tapes have an 3.5-inch form factor. The first generation provide 20 GB (native) and 40 GB (with 2:1 compression) capacity on a single 8 mm data cartridge. The maximum data transfer rates were 3 MB/s uncompressed and 6 MB/s (with 2:1 compression).

With the Mammoth-2 technology the capacity and data rate have been increased to 60 GB (120 GB with 2:1 compression) and 12 MB/s uncompressed (24 MB/s with 2:1 compression). Mammoth-2 drives are read compatible with the previous models.

Advanced Intelligent Tape (AIT) format

The AIT format was developed by Sony. Available in a 3.5-inch form factor, Sony's AIT-1 drives and media provide 25 GB (native) and 50 GB (with 2:1 compression) capacity on a single 8 mm data cartridge. The maximum data transfer rate is 3 MB/s native.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1462
Doc: 3690



With the AIT-2 technology made available in 1999, the capacity and data rate have been increased to 50 GB (100 GB with 2:1 compression) and 6 MB/s native. AIT-2 drives are backward-compatible with the AIT-1models.

Sony's latest AIT-3 format, made available in 2001, doubles the capacity and performance of the prior generation to 100 GB (200 GB with 2:1 compression) and 12 MB/s native. AIT-3 drives are backward-compatible with the AIT-2 and AIT-1 models.

AIT drives feature an Auto Tracking Following (ATF) system, which provides a closed-loop, self-adjusting path for tape tracking. This servo tracking system adjusts for tape flutter, allowing data tracks to be written much closer together for high-density recording. AIT provides Fast/Wide SCSI technology with data transfer rates of up to 12 MB/s (native), 24.0 MB/s (with 2:1 compression). AIT uses the Adaptive Lossless Data Compression technology (ALDC) compression algorithm. The 8 mm standard has various drive generations, all of which are backward-compatible, shown in Table 3-3.

Table 3-3 Standards for 8 mm

Standard	Capacity	Maximum Data Transmission Rate (compressed)
Standard 8 mm	3.5/7 GB	0.53 MB/s
Standard 8 mm	5/10 GB	1 MB/s
Standard 8 mm	7/14 GB	1 MB/s
Standard 8 mm	7/14 GB	2 MB/s
Mammoth	20/40 GB	6 MB/s
Mammoth-2	60/120 GB	24 MB/s
AIT-1	25/50 GB	6 MB/s
AIT-2	50/100 GB	12 MB/s
AIT-3	100/200 GB	24 MB/s

3.1.6 Digital Linear Tape (DLT)

DLT drives appeared in 1985 when Digital Equipment Corporation needed a backup system for their MicroVAX systems.

The system uses a square cartridge that contains tape media but no take-up reel. The take-up reel was built into the drive itself. This design eliminated the additional space typically associated with cassette and cartridge drives such as

QIC or 8 mm. The drive itself had to be made larger than most to accommodate the internal take-up reel. Called the TK50, the new tape drive was capable of storing 94 MB per cartridge.

Using a ferrite read/write head, the TK50 recorded data in linear blocks along 22 tracks. The TK50's read/write head actually contained two sets of read/write elements. One set was used when reading and writing forward, and the other when reading and writing backward.

The TK50 started recording at the beginning of the tape, recording on one track. When it reached the end, the system recorded back to the beginning along a new track. After every two tracks that were written, the system moved the head up the width of one track and began the process again. The read-after-write capability of the system ensured basic data accuracy. The drive fit into a full-height, 5.25" drive bay.

In 1987, Digital released the TK70. This tape drive offered 294 MB of storage on the same square tape cartridge, a threefold improvement over the TK50. This was accomplished by increasing the number of tracks to 48 and by increasing density on the same 1/2-inch tape.

In 1989, Digital introduced the TF85, the first true DLT system. The TF85 (later to be called the DLT 260) incorporated a new feature that enabled the system to pack 2.6 GB onto a 1,200-foot tape (CompacTape III, now known as DLTtape III).

The DLT Tape Head Guide Assembly was incorporated for the first time in the TF85 drive. Six precision rollers provided long tape life. The six-roller head guide assembly gave the TF85 a much shorter tape path than helical-scan systems (Figure 3-6).

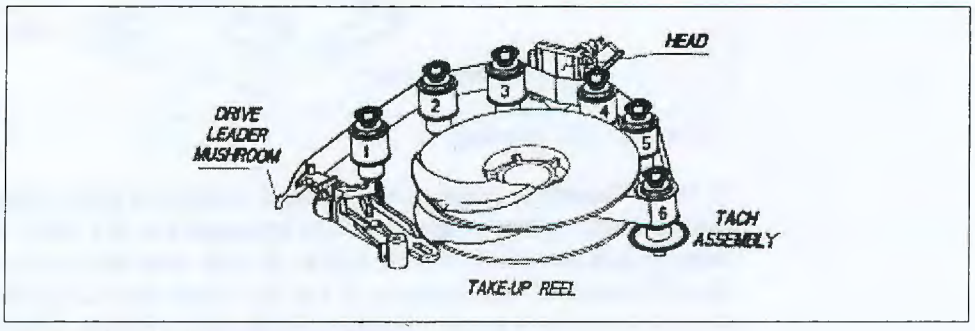


Figure 3-6 DLT tape path mechanism

The read/write head was equipped with an additional write element. The elements now were arranged in a write/read/write pattern. This pattern enabled

TRT 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1463
Doc: 3690

the TF85 to read after writing on two channels and in both forward and reverse directions. This is the multi-channel serpentine recording depicted in Figure 3-7.

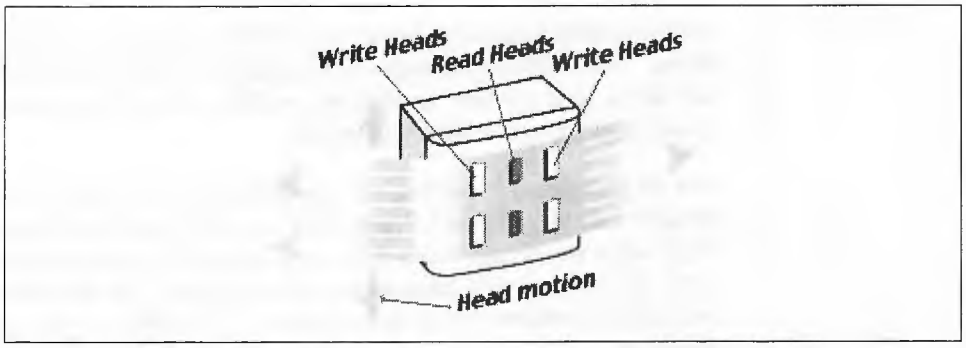


Figure 3-7 DLT 2000 recording head design

Two years later, Digital introduced the TZ87, now known as the DLT 2000 tape drive. This system offered 10 GB of native capacity on a single CompacTape III cartridge (shown in Figure 3-8) and now known as DLTtape III, 2 MB of read/write data cache memory, and a data transfer rate of 1.25 MB/s. This was the first generation of DLT.

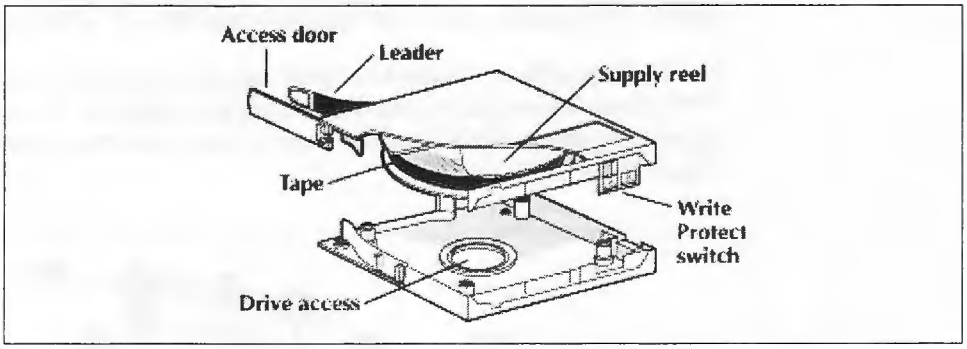


Figure 3-8 DLT cartridge

In 1994, Quantum acquired the Storage division of DEC (Digital Equipment Corporation). In late 1994, Quantum released the DLT 4000. By increasing real density (bits per inch) from 62,500 to 82,000, and tape length by 600 additional feet (DLTtape IV), the capacity of the DLT 4000 grew up to 20 GB (40 GB compressed) on a single 1/2-inch DLTtape IV cartridge. The new DLTtape system provided data transfer at 1.5 MB/s (3 MB/s compressed) and was fully read/write compatible with previous generations of DLTtape drives.

DLT 2000 and DLT 4000 drives write data on two channels simultaneously in linear tracks that run the length of the tape, as shown in Figure 3-9 on page 61.

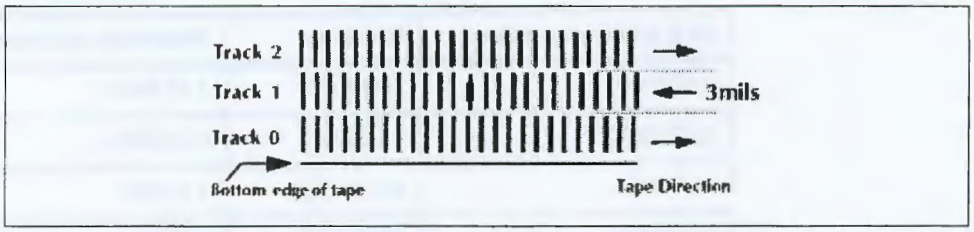


Figure 3-9 DLT 2000/4000 linear recording format

The DLT 7000 appeared in 1996. This drive offered a total storage capacity of 35 GB native, 70 GB compressed on the 1,800 foot DLTtape IV cartridge. The DLT 7000 incorporated a 4-channel head that gives the drive a transfer rate of 5 MB/s of data in native mode (Figure 3-10).

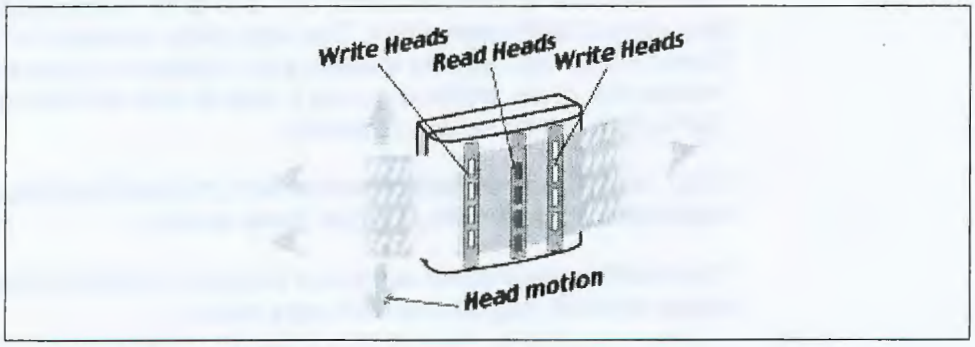


Figure 3-10 DLT 7000/8000 tape head

Quantum's latest DLT product is their DLT 8000 drive. This tape drive features a native transfer rate of up to 6 MB/s, with a native capacity of 40 GB. The DLT 7000/8000 drives incorporate the Symmetric Phase Recording technology that writes data in an angled pattern (Figure 3-11).

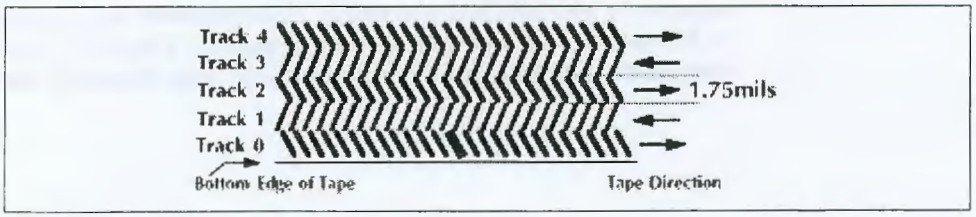


Figure 3-11 Symmetric Phase Recording technology

The DLT standard has various generations of tape drive, all of which are backward-compatible. We have summarized the specifications in Table 3-4 on page 62.

CPMI - CORREIOS
Fls Nº 1464
Doc: 3690

Table 3-4 DLT drive standards

DLT drive generation	Capacity	Maximum data transmission rate
DLT2000	10/20 GB	1.25 MB/s
DLT2000XT	15/30 GB	1.25 MB/s
DLT4000	20/40 GB	1.5 MB/s
DLT7000	35/70 GB	5 MB/s
DLT8000	40/80 GB	6 MB/s

3.1.7 SuperDLT (SDLT)

SuperDLT (SDLT) is a new format specification designed by Quantum Corporation as an evolution of the DLT standard. It uses Laser Guided Magnetic Recording (LGMR) technology. This technology includes the Pivoting Optical Servo (POS). This optically assisted servo system is implemented on the unused reverse side of the media and uses a laser to read the servo guide. SDLT uses 100% of the media for data recording.

SDLT uses Advanced Metal Powder (AMP) media containing embedded information for the Pivoting Optical Servo system.

The recording mechanism is made of Magneto-Resistive Cluster (MRC) heads, a cluster of small magneto-resistive tape heads.

The first SDLT drive, the SDLT 220, was introduced in late 2000. It provides a capacity of 110 GB (native) and 220 GB (with 2:1 compression). The native data transfer rate is 11 MB/sec. This first drive was not backward-read-compatible with earlier models. In 2001 Quantum released a version of the SDLT 220 drive that was backward-read-compatible with the DLTtape IV cartridge.

Quantum's latest SDLT 320 drive came available in 2002. It increased the native capacity to 160 GB (320 GB with 2:1 compression) and the native transfer rate to 16 MB/sec (32 MB/sec with 2:1 compression). The SDLT 320 is backward read compatible with DLTtape IV cartridges and uses Super DLTtape I media.

3.1.8 IBM 3480

The second generation of IBM magnetic tapes and the first one to use an enclosed cartridge containing 1/2-inch tape, the IBM 3480, was announced on March 22, 1984. The tape was stored in a now-familiar cartridge, which was smaller, much more robust, and easier to handle than tape reels. The cartridge capacity was 200 MB, and the channel data rate was 3 MB/s, writing 18 tracks in one direction.

3.1.9 IBM 3490

The 3490 replaced the 3480 tape technology, using the same tape cartridge media. The IBM 3490E, with a tape capacity of 800 MB uncompacted (2.4 GB compacted) and a channel data rate of 3 MB/s, increased the capacity of the 3480 fourfold by using a double-length tape and by writing data in both directions: 18 tracks to the end of tape, and 18 tracks back to the start of the tape.

During this second generation, several steps were taken to automate tape processing and to reduce or eliminate human intervention. Automatic cartridge loaders and automated tape libraries, such as the StorageTek Silos and the IBM 3495 and 3494 libraries, were introduced to reduce or eliminate the need for tape operators. Software packages, such as CA-1, TLMS, and the DFSMS Removable Media Manager (DFSMSrmm™), were implemented to manage the tape volumes automatically.

The IBM 3490 and compatible drives were probably the first family of tape products that were mostly used with automatic tape libraries rather than being installed as stand-alone drives operated manually.

Applications still used tapes directly, and the Improved Data Recording Capability (IDRC), which compacts the data, reduced the number of tape volumes used.

Magnetic disks were now widely used for online data, and these second-generation tape systems therefore became primarily a medium for backup and were introduced as an archive medium. The process of archiving was also automated with products such as Hierarchical Storage Manager (HSM) and DFSMShsm™ (a component of DFSMS/MVS®) using tape as the lowest level in a storage hierarchy. Of course, tape was still used as an interchange medium, but networks were also used for that purpose.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1465
3690
Doc:

3.1.10 IBM Magstar 3590

IBM Magstar tape technology was first introduced in July 1995. The original cartridge maintained the external form factor of the 3490 (Figure 3-12), had a capacity of 10 GB uncompacted (30 GB compressed), and the data rate was 9 MB/s. Later drive models and new media increased these figures. The data format is not compatible with the 3490.

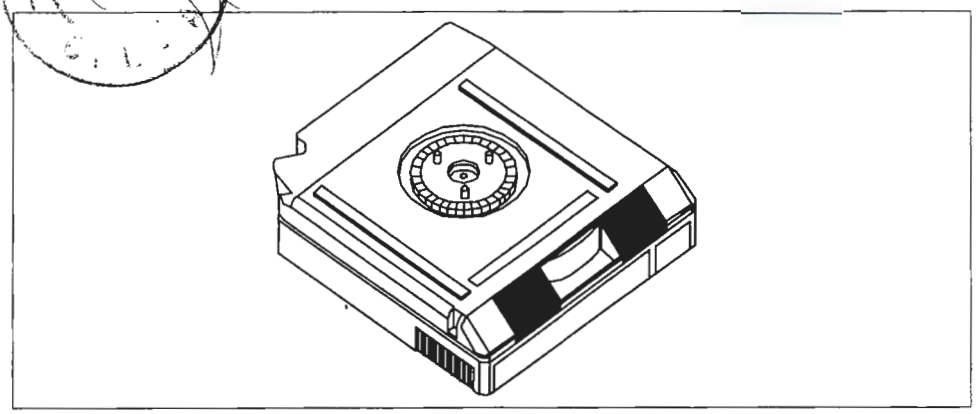


Figure 3-12 Magstar 3590 tape cartridge

The Magstar 3590 drive (see Figure 3-13 on page 65) incorporates a new longitudinal technology, Serpentine Interleaved Longitudinal Recording. Data is written in each direction in turn, and to increase capacity further by providing multiple sets of tracks in parallel, the concept of *head indexing* is introduced. The entire set of heads is slightly shifted after one pass, and all subsequent passes (for a total of eight) are used to write data tracks adjacent to the existing ones. This means a significant improvement in the tape capacity and transfer rates without changing the tape speed (2 m/s) and media length (600 m). A buffer is used, and the data is compressed before it is written to tape. In addition, the drive can complete a stop-start cycle in approximately 100 ms. The performance is significantly improved for both start-stop and streaming applications.

With the IBM TotalStorage Enterprise Magstar 3590 Model H and the Extended Length Cartridges made available in 2002, the capacity and data rate have been increased to 60 GB (180 GB assuming 3:1 compression) and 14 MB/s native respectively, while maintaining backward compatibility for reading with the base models.

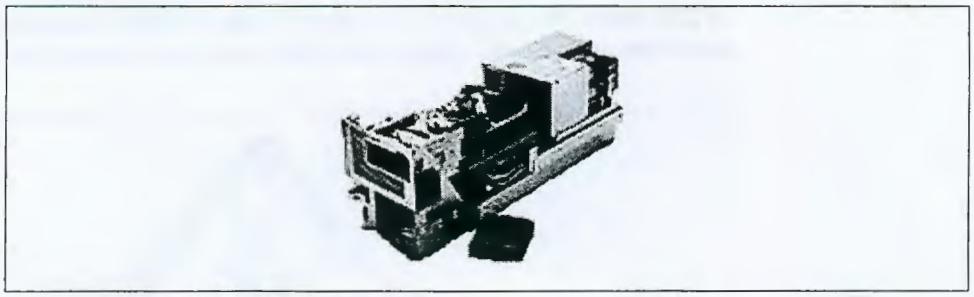


Figure 3-13 Magstar 3590 tape drive

This design incorporates some innovations such as servo tracks on the tape to guide the read/write heads along the data tracks and the implementation of an improved error correcting code (ECC). A portion of the tape within each cartridge is reserved for statistical information; it is continually updated after each read or write, providing statistics that can be used to obtain drive and media information and identify problems with a particular tape or drive as early as possible.

Metal particle media

A chromium dioxide medium was used in the IBM 3480 and 3490 cartridges. The IBM 3590 High Performance Tape Cartridge uses a metal particle medium, which has a significantly increased coercivity and therefore permits a much higher data recording density in comparison with chromium dioxide media. The linear density is proportional to the medium's coercivity, and therefore the linear density of the IBM 3590 tape is approximately three times that of the IBM 3480 and 3490. The track density is also improved approximately fourfold. Advances in the metal particle coatings and media binders afford reliability and magnetic stability equal or superior to chrome media.

3.1.11 STK 9840

Introduced in late 1998, the STK T9840 tape drive (dubbed "Eagle") is based on linear technology and targeted at the high-end, enterprise server market. The dual-hub cartridge (shown in Figure 3-14 on page 66) has a native capacity of 20 GB and a maximum data rate of 10 MB/s. To maintain compatibility with existing enterprise system automation products (mainly the STK silos), the cartridge maintains the external form factor of the 3490/3590 cartridge.

In 2001, StorageTek introduced a second-generation 9840 drive, the T9840B. Tape speed during read/write operations doubled, from 2 m/sec on the T9840A to 4 m/sec on the T9840B, and maximum data transfer rate nearly doubled, to 19 MB/sec. The capacity is still 20 GB (native) and 40 GB (with 2:1 compression).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1466
3690
Doc:

Data on both drives is written 16 tracks at a time in a total of 18 passes, for a total of 288 tracks. In addition to the data tracks, the tape contains five bands of five servo tracks each (25 tracks total) that are pre-written on the tape.

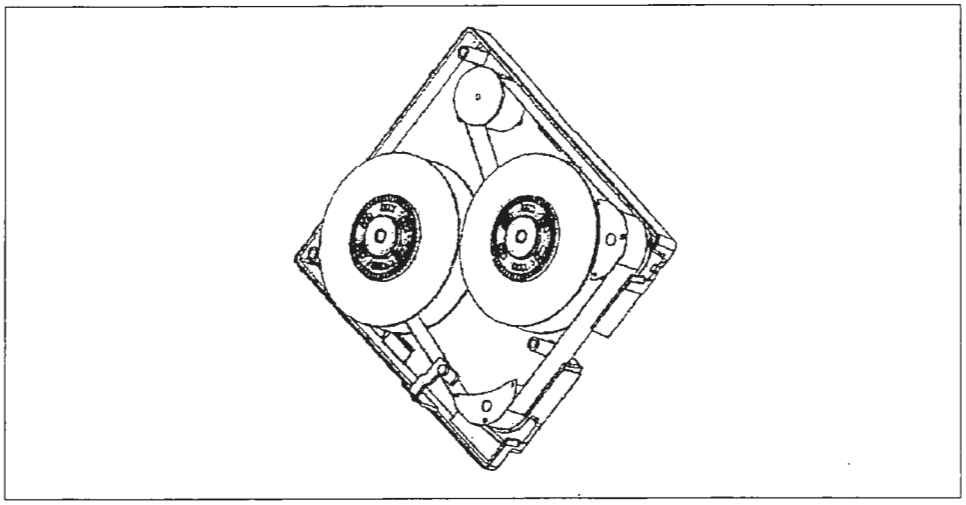


Figure 3-14 STK 9840 tape cartridge

3.1.12 STK 9940

The STK T9940 is based on T9840 technology. The biggest differences between these two drives are the data cartridge and the loader mechanism for the cartridge. TheT9940 cartridge has the same form factor and dimensions as the T9840 cartridge, but the T9940 cartridge contains a single reel of media, and the tape path, take-up reel, and tape guidance system are located inside the drive. The first-generation T9940A drive has a capacity of 60 GB (native) and 120 GB (with 2:1 compression). The native data transfer rate is 10 MB/sec.

The StorageTek T9940B format, made available at the end of 2002, increased the capacity and data transfer rate of the prior generation to 200 GB (400 GB with 2:1 compression) and 30 MB/s native. the T9940B drive is backward-read-compatible with the T9940A model.

3.1.13 LTO Ultrium

The Linear Tape-Open (LTO) standard was released as a joint initiative of IBM, Hewlett-Packard, and Seagate Companies. As result of this initiative, two LTO formats (Ultrium and Accelis) were defined.

The consortium of these companies is known as the Technology Provider Companies. The new technology specifications are detailed at an LTO Web site:

`http://www.lto-technology.com`

The IBM LTO Ultrium 1 drive provides a single-media capacity of up to 100 GB (200 GB with 2:1 compression) data storage per cartridge and a sustained data rate of up to 15 MBps (uncompressed), while the newly released IBM LTO Ultrium 2 drive has doubled media capacity to 200 GB (400 GB with 2:1 compression) data storage per cartridge and more than doubled sustained data rate to 35 MBps (uncompressed).

For a detailed description of the LTO Ultrium tape format specification, see 1.2.2, "LTO core technology" on page 6.

For a detailed description of the IBM LTO Ultrium drive, see 2.4, "IBM LTO Ultrium common subassembly" on page 28.

3.1.14 Libraries

System administrators are clamoring for technologies that enable them to efficiently and economically manage the explosive growth in stored data. As the amount of data increases, the backup process takes longer and longer.

The solution to this problem is to use a device that integrates the tape drive with some level of automation. The challenge is to choose the right solution in terms of size and automation level.

System administrators industry-wide have recognized the need for automating the backup-and-restore process to the extent that little or no human intervention is required. This has come to be known as *lights-out backup*. This process can be done off-shift, or concurrently with other applications during normal operations. Multi-drive tape libraries are the only available technology that offer both the reliability and low cost to make lights-out backup practical.

The hardware options for automation are autoloaders and a range of multi-drive automated tape libraries. We distinguish between them below.

Autoloaders

Autoloaders have one tape drive and typically are used to access a small number of tapes once a day. Most are designed for purely sequential operations. These units place no emphasis on performance.

ECT/ECT n° 03/2005 - CN - CPMI - CORREIOS
Fls N° 1467
Doc: 3690

Automated tape libraries

Automated tape libraries have one or more tape drives, but typically are used with at least two tape drives. All tape cartridges are accessible to all drives, thus making concurrent reading and writing operations possible.

Throughput can be increased by adding additional drives. Libraries can exchange tapes in a few seconds, substantially improving file-restore response times. Tape libraries are mandatory for lights-out operations and other higher performance tape storage applications. Tape libraries also offer the security of knowing that other drives will take over if one should fail.

Multi-drive automated tape libraries and ultra-scalable tape libraries combined with storage-management software, including concurrent backup, archive, and HSM, offers the most robust solution to manage and protect huge amounts of corporate data. Automated tape libraries allow random access to large numbers of tape cartridges and concurrent use of two or more drives, rather than manually loading one tape after another or using a single-drive sequential autoloader.

Enterprise tape libraries

Enterprise tape libraries are automated tape libraries that provide enhanced levels of automation, scalability, reliability, availability and serviceability. They typically have the capacity to house dozens of drives and hundreds of tapes. Equipped with high-performance robotic mechanisms, bar code scanners, and support for cartridge I/O ports, these libraries often offer redundant components and a high degree of flexibility through a modular design. Some models add support for multiple SCSI, FC-AL, FCP, and ESCON®, or FICON™ connections to allow connection to more than one host platform. At the top of the line of the enterprise tape libraries are products such as the IBM TotalStorage Enterprise Tape Library 3494 and the IBM TotalStorage UltraScalable Tape Library 3584 that are designed to be shared between two or more heterogeneous host systems. All the hosts have access to the control functions of the tape library robotics. Simply put, the library is shared in a physical way, with each system thinking it really owns the entire library.

3.2 Current SAN technologies

A SAN (Storage Area Network) is a high-speed network that enables the establishment of direct connections between storage devices and processors (servers) within the distance supported by Fibre Channel.The SAN can be viewed as an extension to the storage bus concept that enables storage devices and servers to be interconnected using elements similar to Local Area Networks (LANs) and Wide Area Networks (WANs): routers, hubs, switches, directors, and

gateways. A SAN can be shared between servers or dedicated to one server. It can be local or extended over geographical distances.

In today's SAN environment the storage devices in the bottom tier are centralized and interconnected, which represents, in effect, a move back to the central storage model of the host or mainframe.

Figure 3-15 shows a tiered overview of a SAN connecting multiple servers to multiple storage systems.

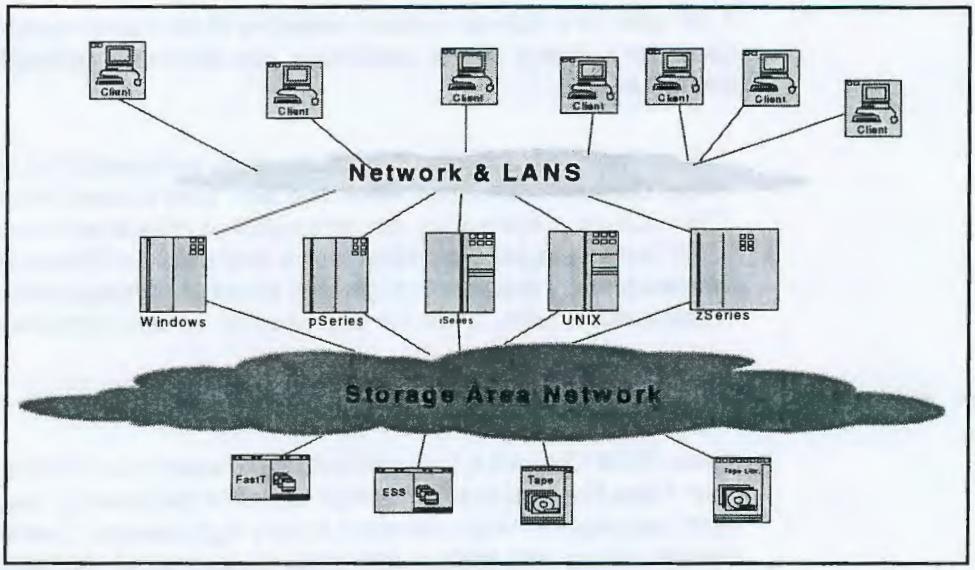
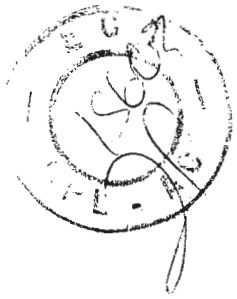


Figure 3-15 Overview of a SAN

A SAN facilitates direct, high-speed data transfers between servers and storage devices, potentially in any of the following three ways:

- Server to storage: This is the traditional model of interaction with storage devices. The advantage is that the same storage device may be accessed serially or concurrently by multiple servers.
- Server to server: A SAN may be used for high-speed, high-volume communications between servers.
- Storage to storage: This outboard data movement capability enables data to be moved without server intervention, thereby freeing up server processor cycles for other activities such as application processing. Examples include a disk device backing up its data to a tape device without server intervention, or a remote device mirroring across the SAN.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1468
Doc: 3690



3.2.1 SAN definition

The Storage Network Industry Association (SNIA) defines SAN as a network whose primary purpose is the transfer of data between computer systems and storage elements and among storage elements. A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage elements, and computer systems so that data transfer is secure and robust. The term SAN is usually (but not necessarily) identified with block I/O services rather than file access services.

It can also be a storage system consisting of storage elements, storage devices, computer systems, and/or appliances, plus all control software, communicating over a network.

Note: The SNIA definition specifically does not identify the term SAN with Fibre Channel technology. When the term SAN is used in connection with Fibre Channel technology, use of a qualified phrase such as *Fibre Channel SAN* is encouraged. According to this definition, an Ethernet-based network whose primary purpose is to provide access to storage elements would be considered a SAN. SANs are also used for system interconnection in clusters.

3.2.2 Fibre Channel architecture

Today, Fibre Channel is the architecture on which most SAN implementations are built. Fibre Channel is a technology standard that enables data to be transferred from one network node to another at very high speeds. Current implementations transfer data at 100 MB/s or 200 MB/s. Data rates of 1000 MB/s have been tested and many companies have products in development that will support this. The Fibre Channel standard is accredited by many standards bodies, technical associations, vendors, and industry-wide consortia. There are many products on the market that take advantage of its high-speed, high-availability characteristics.

Fibre Channel was completely developed through industry cooperation, unlike SCSI, which was developed by a vendor and submitted for standardization after the fact.

Note: The word *Fibre* in Fibre Channel is spelled in the French way rather than the American way because the interconnections between nodes are not necessarily based on fiber optics, but could be based on copper cables. It is also the ANSI X3T11 technical committee's preferred spelling. This is the standards organization responsible for Fibre Channel and certain other standards for moving electronic data in and out of computers. Even though copper-cable-based SANs are rare, the spelling has remained.

3.2.3 Topologies

Fibre Channel interconnects nodes using three physical topologies that can themselves have variants. These topologies are:

- Point-to-point: The point-to-point topology consists of a single connection between two nodes. All of the bandwidth is dedicated for these two nodes.
- Loop: In the loop topology, the bandwidth is shared between all the nodes connected to the loop. The loop can be wired node-to-node; however, if a node fails or is not powered on, the loop is out of operation. This is overcome by using a hub. A hub opens the loop when a new node is connected and closes it when a node disconnects. A major drawback in this technology is the Loop Initialization Process (LIP), which needs to occur every time a node is removed from the loop or a new node is added to the loop. The LIP process disrupts the loop and can cause data disruptions.
- Switched: A switch enables multiple concurrent connections between nodes. This is generally referred to as a switched fabric. Switched fabric is more reliable than a loop because there is no need for the LIP process. New nodes can be added and removed without any disruption to the Fibre Channel processes.

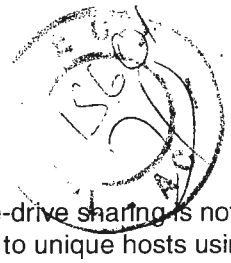
3.2.4 Tape solutions in a SAN environment

Connectivity to tape is essential for most backup processes. However, manual tape operations and tape handling are expensive. Studies show that automation of tape processing saves money and increases reliability. Enterprises have long had to utilize staff to remove these tapes, transport them to a storage site, and then return them to the tape drive for mounting when needed. Customer tape planning initiatives are directed at more efficient utilization of drives and libraries, as well as minimization of manual labor associated with tape processing.

The biggest issues with SCSI tape implementations are the limited cable length and the limited possibilities to share drives between several systems. For LVD SCSI the total cable length is limited to 25 m using point-to-point interconnection (such as one host connected to only one tape drive). With multi-drop interconnection (one host connected to more than one tape drive on the same SCSI bus) the total cable length is 12 m for LVD SCSI and 25 m for HVD SCSI. Most SCSI tape drives currently have only one SCSI port and hence can only be attached on one SCSI bus. This severely limits the number of hosts that can physically allocate the drive without recabling.

SANs enable greater connectivity of the tape libraries and tape drives, as well as tape sharing, which will be discussed later in this chapter. With Fibre Channel the distance between the server (or data point) and the connected tape node can be up to 10 km. Fibre Channel enables multiple host scenarios without recabling.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1469
Fls. Nº
3690
Doc:



If software to manage tape-drive sharing is not available, we would have to isolate (or *zone*) the drives to unique hosts using functions commonly available on SAN gateways or switches. With the proper management software, each drive can talk to each host, and connections can be dynamic without recabling.

Backup solutions can utilize SAN technology in a number of ways to reduce the costs of their implementation and at the same time increase their performance.

Sharing tape devices on a SAN environment

The tape world has three distinct means of sharing:

- Library sharing
- Drive sharing
- Media sharing

Library sharing

Library sharing occurs when multiple servers attached to a tape library share both the library and the robotics. The tape drives within the library may or may not be shared (pooled) among the attached servers. Tape library sharing is a prerequisite for tape-drive sharing.

Drive sharing

The sharing of one or more tape drives between multiple servers is called drive sharing. To share drives between heterogeneous applications within a tape library, the tape library must provide multiple paths to the robotics and also must have the capability to define the library's drives and slots as multiple logical libraries. The server attached to each partition has no knowledge of any drives or slots outside the partition.

Media sharing

Media sharing today is only possible in a homogeneous environment between servers that use the same backup server and the same library to back up their data. For systems that are not backed up by the same backup server it is only possible to share a tape scratch pool.

Figure 3-16 on page 73 shows the multi-path architecture of the 3584 LTO tape library. Every drive can have a path defined to the SCSI Medium Changer (SMC).

The library on the left has been partitioned into three logical libraries. In the AIX and NT partitions, only the first drive has a library control path defined.

The iSeries is unique in that every IOP/IAP has to have a library control path defined. The iSeries attached to the left-hand library has two SCSI buses and therefore, two library control paths defined. These three servers are sharing the 3584 LTO tape library but not the drives.

The library on the right has not been partitioned, and has only one logical library. Every iSeries SCSI bus has a library control path defined to allow control of the 3584 robotics. The iSeries supports the attachment of one Ultrium 1 LTO tape drive and of up to 15 Ultrium 2 LTO tape drives per SCSI bus.

The iSeries Servers attached to the right-hand library are also sharing the library even thoughit has not been partitioned. Through BRMS the iSeries Servers are sharing the library and media, but no tape-drive pooling is being done.

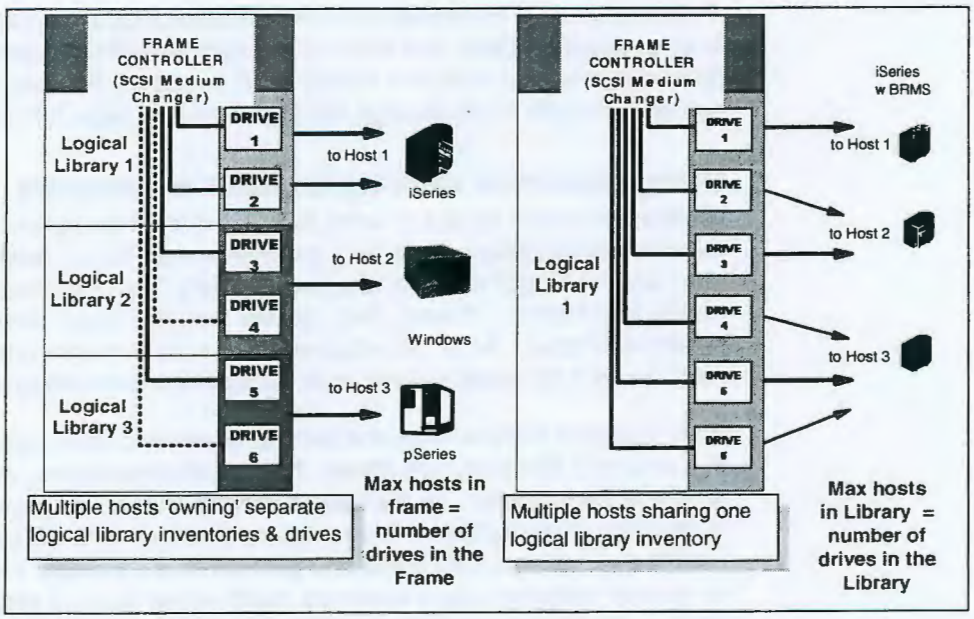


Figure 3-16 IBM 3584 multi-path architecture

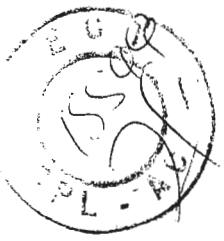
IBM LTO in SAN environment

The new IBM LTO Ultrium 2 Tape Drives are available with a Fibre Channel interface for either point-to-point or Fibre Channel-Arbitrated Loop attachment. These options remove the need to use a SAN data gateway. The device can be attached directly to SAN switches or FC-AL hubs.

For IBM LTO Ultrium 1 Tape Drives, SAN attachment must occur via a SAN data gateway. For drives with LVD interfaces, attachment must be through the SAN Data Gateway Router, 2108-R03. For drives with HVD interfaces, attachment must be through either the SAN Data Gateway Router, 2108-R03, or the SAN Data Gateway for Tape, 2108-G07.

In each case, the server will require a supported Fibre Channel HBA.

RQS nº 03/2005 - CN - CPMI – CORREIOS
Fls. Nº 1470
Doc: 3690



Backup software for SAN environments

Implementing backup solutions in a SAN topology requires software developed to enable the sharing of tape drives at a logical level. The major benefits of this software are:

- Direct connection of the tape drive to the server for high speed
- Sharing the drive with another server to save money

All you need is the proper traffic control feature at a software level.

The development of backup software solutions supporting tape-sharing on SAN is an ongoing process, and many of the back-up software vendors have already delivered products or plan to deliver such a product. IBM has made tape-sharing available for IBM Tivoli Storage Manager since Version 3.7 (October 1999).

Using electronic vaulting for disaster recovery

Another important aspect of using tape in a SAN is the opportunity to exploit tape connectivity for disaster recovery enhancements. Today most enterprises take their tape backups offsite for disaster recovery. The tape is actually created in a locally attached tape library, then ejected from the library, and finally removed to an offsite location. All of this requires manual intervention and is error-prone. A major reason for failed recoveries is caused by a tape being mis-placed.

Fibre Channel SANs enable the backup server to create tapes easily and safely in a remotely attached tape library. This is called electronic vaulting. It removes all of the manual effort, as the tape is already offsite, and prevents a major cause of disaster-recovery failure. Currently, most enterprises staff tape operations to handle the tapes as they come and go from offsite storage. Fibre Channel allows for greater distances, so it becomes much easier to put a remote tape library at another location to create the backup tape copy. With this method, outlined in Figure 3-17 on page 75, no manual handling is necessary.

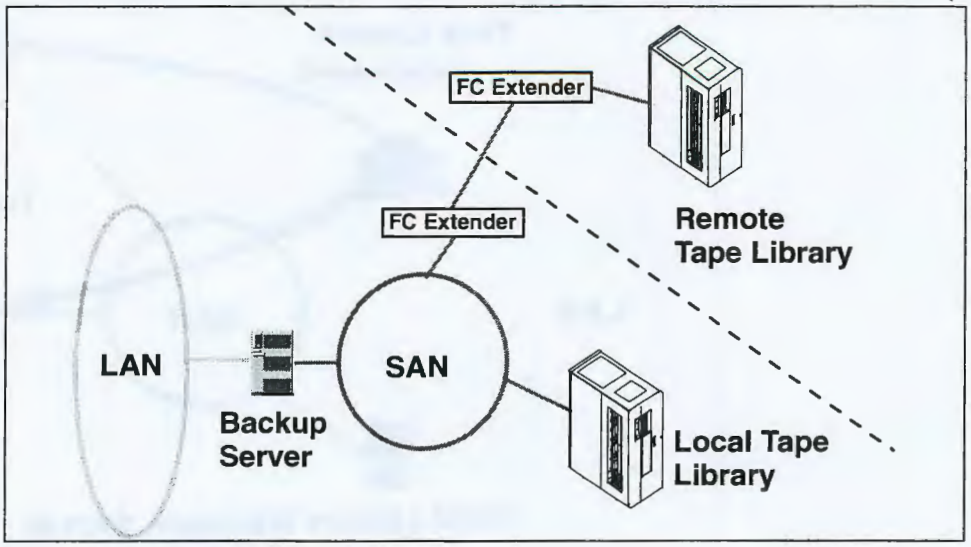


Figure 3-17 Electronic vaulting

LAN-free backup

SAN technology provides an alternative path for data movement between the backup client and the server. Shared storage resources (disk, tape) are accessible to both the client and the server through the SAN. Data movement is off-loaded from the LAN and from the server processor and allows for greater scalability. LAN-free backups decrease the load on the LAN.

Managed System for SAN is a feature of IBM Tivoli Storage Manager that enables LAN-free data movement. The Tivoli Storage Manager client data moves directly to and from a storage device attached to a SAN. A Tivoli Storage Manager storage agent is installed on the client machine and shares storage resources with the Tivoli Storage Manager server. The storage agent can write directly to storage media in a format that is consistent with that used by the server. The Tivoli Storage Manager server or servers controls the storage devices and keeps track of the data that the client has stored. Tivoli Storage Manager continues to use a LAN connection to exchange control information, such as policy information and data about the objects that are backed up. Using the SAN for client data movement decreases the load on the Tivoli Storage Manager server and allows the server to support a greater number of simultaneous client connections. See Figure 3-18 on page 76.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1471
Doc: 3690

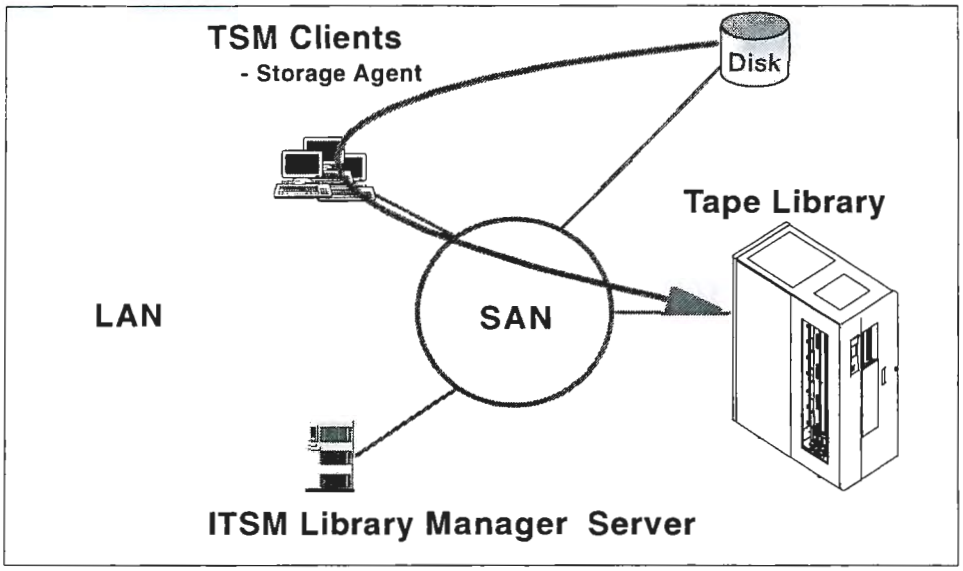


Figure 3-18 Tivoli Storage Manager LAN-free backup

The storage agent communicates with the server via the LAN to obtain and store database information and to coordinate device and volume access. The server determines if the client is requesting access to storage for which the client has a SAN path defined. If a SAN path is defined, the client (by means of the storage agent) transfers data on that path. If a failure occurs on the SAN path, failover occurs and the client uses its LAN connection to the Tivoli Storage Manager server and moves the client data over the LAN.

Server-free backup

Server-free data movement provides a way to back up and restore large volumes of data between client-owned disks and storage devices in a method that reduces overhead on the backup server and the backup client, and that minimizes data transfer on the LAN. This is done by making use of the SCSI–3 extended copy command. The command is issued and initiated by the server and carried out by a data mover device (e.g. SAN Data Gateway) that exists on the SAN. The data mover device is responsible for moving the data either from a SAN-attached client-owned disk to a SAN-attached tape drive, or from a SAN-attached tape drive to a SAN-attached client-owned disk, which frees the server and the client from the operation. The process is shown in Figure 3-19 on page 77.

Server-free backup/restore capability was introduced into IBM Tivoli Storage Manager in Version 5 for certain platforms. For more information on server-free capabilities of Tivoli Storage Manager, see the support page at `http://www-3.ibm.com/software/tivoli/products/storage-mgr-san/platforms.html` and the redbook *IBM Tivoli Storage Manager Version 5.1 Technical Guide*, SG24-6554.

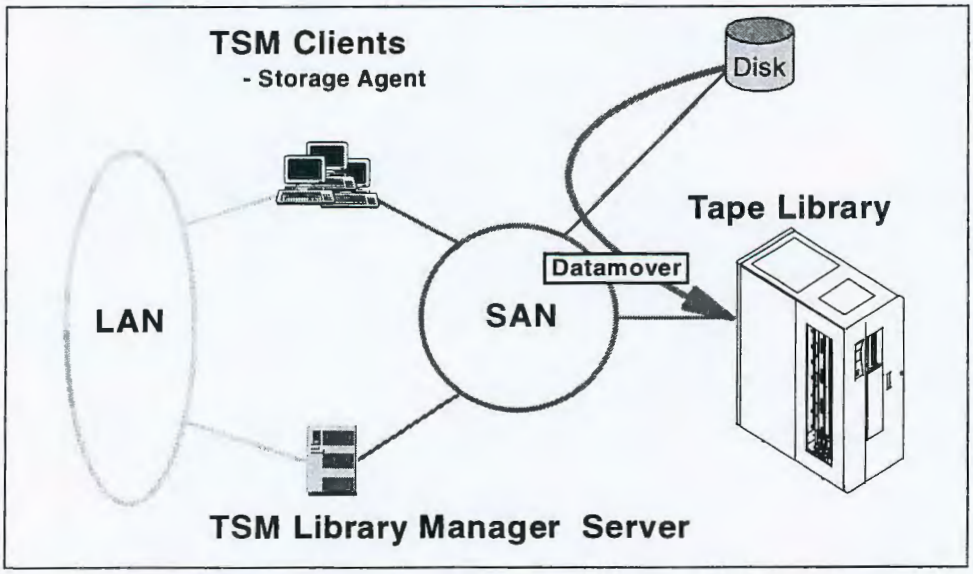


Figure 3-19 Tivoli Storage Manager server-free backup

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1472
3690
Doc:

4

IBM TotalStorage Ultrium Tape Drive 3580

The IBM TotalStorage Ultrium Tape Drive 3580 is the smallest in the family of IBM Ultrium tape solutions. It is an external, stand-alone, SCSI-attached tape drive that attaches to iSeries, pSeries, xSeries, RS/6000® SP, and other UNIX and PC servers supporting OS/400®, IBM AIX, Sun Solaris™, HP-UX, Microsoft Windows NT, Microsoft Windows 2000, Microsoft Windows 2003, and Red Hat and SuSE Linux using a suitable SCSI adapter.

The IBM 3580 Ultrium tape drive is a very cost-effective solution for save-and-restore and archiving functions, and it provides an excellent migration path from SDLT, 1/4-inch, 4 mm, or 8 mm tape drives.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1473
Doc 3690

4.1 Model description

The IBM 3580 is a large-capacity, high-performance Ultrium tape drive available as six separate model types, depending on the capacity and SCSI[1] interface required.

Figure 4-1 IBM 3580 model L11/L13/L23 or H11/H13/H23 Ultrium tape drive

There are six model types:

- *IBM 3580-L11* and *IBM 3580-L13* have 100GB native capacity with a Low-Voltage Differential (LVD) Ultra2 SCSI attachment that connects to LVD fast/wide adapters.
- *IBM 3580-H11* and *IBM 3580-H13* have 100GB native capacity with a High-Voltage Differential (HVD) Ultra SCSI attachment that connects to HVD fast/wide adapters.
- *IBM 3580-L23* has 200GB native capacity with a Low-Voltage Differential (LVD) Ultra2 SCSI attachment that connects to LVD fast/wide adapters.
- *IBM 3580-H23* has 200GB native capacity with a High-Voltage Differential (HVD) Ultra SCSI attachment that connects to HVD fast/wide adapters.

The IBM 3580 models L11, L13, H11, and H13 all use the Ultrium 1 LTO cartridge, which has a capacity of 100GB (200GB with 2:1 compression), and are capable of sustaining a data rate of up to 15 MB/s (uncompressed).

[1] Refer to 2.4.3, "Interfaces" on page 31 for an explanation of HVD and LVD.

The IBM 3580-L11 and IBM 3580-L13 are functionally identical. The only difference is that the IBM 3580-L13 has a three-year Customer Element Exchange warranty. The IBM 3580-H11 and IBM 3580-H13 are functionally identical; the only difference is that the IBM 3580-H13 has a three-year Customer Element Exchange warranty.

The IBM 3580-L23 and H23 use the Ultrium 2 LTO cartridge, which has a capacity of 200GB (400GB with 2:1 compression), and are capable of sustaining a data rate of up to 35 MB/s (uncompressed).

Note: Although the IBM 3580 Ultrium tape drive provides the capability for high tape performance, other components of the system may limit the actual performance achieved. Also, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

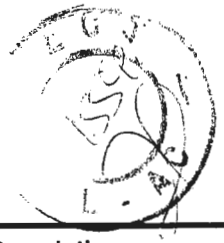
4.2 Feature codes

The IBM 3580 Ultrium tape drive can be ordered with the following feature codes (Table 4-1). We have not included the various cabling options; refer to the product publications for detailed information about configuring and ordering it.

Table 4-1 IBM 3580 feature codes

Feature code	Description	Comments
1748	Custom QuickShip	
8001	One 100GB data cartridge	Plant only; see Media section for details.
8101	One 200GB data cartridge	Plant only; see Media section for details.
8002	One cleaning cartridge	Plant only; see Media section for details.
8723	Rack mount kit	
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9215	Attached to Linux	

RCIS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1474
Doc: 3690



Feature code	Description	Comments
9400	Attached to AS/400®	
9600	Attached to AIX	

4.3 SCSI attachment

The SCSI interface (HVD or LVD) on each IBM 3580 Ultrium tape drive is chosen by selecting the appropriate model number (model H11/13/23 or L11/L13/23).

The IBM 3580 Ultrium tape drive can be attached to IBM pSeries, IBM xSeries, IBM RS/6000 SP systems, IBM iSeries, AS/400, and non-IBM servers, workstations, and personal computers that support Ultra/Wide SCSI HVD and Ultra2/Wide SCSI LVD interface specifications. The interface you choose will depend on the available adapter in the host, which must be of the same type as the drive interface.

The IBM 3580 Ultrium tape drive also may be compatible with other servers, operating systems, and SCSI adapters. Contact your local IBM representative for a current list of supported open system configuration and software vendors or visit `http://www.ibm.com/storage/lto`.

4.4 SCSI cabling

A SCSI cable is required for each IBM 3580 connection to a SCSI bus. A single 2.5 m SCSI cable is available as a no-charge feature; if an alternate length is required it should be included in the initial order. A SCSI terminator is included with each drive.

An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) also may be required for attachment to particular server adapters.

4.4.1 Cables

A single SCSI cable is available as a no-charge feature (either #9702 or #9703) specified only with the initial IBM 3580 order. It is not orderable as a miscellaneous equipment specification (MES) for installation later. Feature #9702 supplies a 2.5 m universal SCSI cable with HD68 connectors at each end; feature #9703 supplies a VHDCI connector at one end and HD68 at the other.

Additional SCSI cables are available as optional features on the IBM 3580 for LVD and HVD attachment to host adapters.

The following cables have an HD68 connector at each end:

- Feature #5301, 0.4 m (1.4 feet) SCSI cable
- Feature #5302, 2.5 m (6.6 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The following cables have a VHDCI connector at one end and an HD68 connector at the other end:

- Feature #5602, 2.5 m (6.6 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 25 m (82 feet) SCSI cable

4.4.2 Interposers

An interposer may be required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries adapter #6501.
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable. The interposer (a 0.3 m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

4.4.3 SCSI length limitations

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection. If using multi-drop interconnection, then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using point-to-point or multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1475
3690
Doc:

4.5 Upgrades

The IBM 3580-L11/L13 and IBM 3580-H11/H13 cannot be upgraded to IBM 3580-L23 and IBM 3580-H23, respectively.

IBM 3580 drives cannot be installed into IBM 3581, 3582, 3583, or 3584 units.

4.6 Environmental specifications

The IBM 3580 is designed to be placed on or beside the attached host server or installed in a standard 19-inch rack.

4.6.1 Physical dimensions

The IBM 3580 is a relatively small single tape drive enclosure:

- Width: 17.1 cm (6.75 in)
- Depth: 33.3 cm (13.1 in)
- Height: 14.6 cm (5.75 in)
- Maximum weight: 6.6 kg (14.3 lbs)

4.6.2 Operating environment

The IBM 3580 can be installed in a normal office environment and does not need to be in a specialized machine room. Refer to the product publications for specific information.

4.7 Host platforms and device drivers

The following no-charge specify codes indicate the server platform to which the IBM 3580 Ultrium tape drive is attached:

- #9210, attached to HP-UX
- #9211, attached to Sun System
- #9212, attached to Windows NT or Windows 2000 System
- #9213, attached to other non-IBM system
- #9215, attached to Linux system
- #9400, attached to AS/400 System
- #9600, attached to RS/6000

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3580). Sometimes the driver code is supplied as part of the operating system code (for example, in

OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

Ultrium 1

The IBM 3580 is shipped with device drivers to support Ultrium 1 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.2 or later
- Sun Solaris 2.6, 7, and 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- HP-UX 11.0
- OS/400 V4R4

Ultrium 2

The IBM 3580 is shipped with device drivers to support Ultrium 2 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.3, 5.1
- Sun Solaris 7, 8, and 9
- Windows NT 4.0 with Service Pack 6
- Windows 2000 (build 2195)
- Windows 2003
- HP-UX 11.0, 11i
- OS/400 V5R1, V5R2
- Linux Red Hat 7.2 (32 and 64 bit kernels), Red Hat 7.3, Red Hat Advanced Server 2.1, SuSE Linux Enterprise Server Update

Tip: The device driver CD or diskette that is shipped with the IBM 3580 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Always check the following FTP site for the latest device drivers:

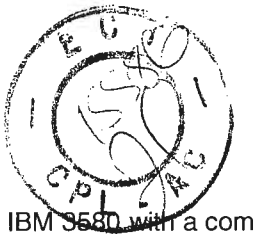
`ftp://ftp.software.ibm.com/storage/devdrvr/`

4.7.1 Device driver installation

Install the IBM device drivers for the IBM 3580 as follows:

- If you intend to use the IBM 3580 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3580.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1476
Doc: 3690



- If you do not intend to use the IBM 3580 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide* GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3580 with a commercial software application, IBM recommends that you install any IBM supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples of using the Ultrium drives are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

4.8 Storage applications

The software to manage the IBM 3580 Ultrium tape drive is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software providers. A list of compatible software is available at the Web site:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium support and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more detailed information of specific versions and platforms supported.

4.9 Performance considerations

For best performance, it is recommended to attach only one tape drive per SCSI bus. This may not be a realistic objective, but minimizing the number of devices per bus will improve performance. Attaching other SCSI devices on the same SCSI bus as the IBM 3580 Ultrium tape drive may affect performance of those devices.

iSeries configurators allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape drive on an input/output port may affect system performance.

Although the compression technology can increase the amount of data stored on the media, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

4.10 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each IBM 3580 drive order[2]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3580:

- Feature #8001 provides a single 100 MB Ultrium 1 Data Cartridge. It is a chargeable feature, and a maximum of five can be ordered.
- Feature #8101 provides a single 200 MB Ultrium 2 Data Cartridge. Additional cartridges can be ordered using part number #08L9870.
- Feature #8002 provides a single Ultrium Cleaning Cartridge. It is a chargeable feature, and a maximum of three can be ordered.

Subsequent to the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about how to order supplies and cartridges, with or without labels.

4.11 IBM 3580 Ultrium tape drive initial set-up

This section covers some of the major items required to implement, manage, and operate the IBM 3580 tape drives. It does not cover all of the tasks, nor do we intend to cover all the specific commands. For more details, refer to *IBM 3580 Ultrium Tape Drive Setup, Operator and Service Guide*, GA32-0415, *IBM TotalStorage LTO Ultrium 2 Tape Drive 3580 Setup and Operator Guide*, GA32-0460, and the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268 and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

4.11.1 SCSI ID

If you attach multiple IBM 3580 SCSI devices in the same chain, they should each use different SCSI IDs starting with the lowest number on the first device as depicted in Figure 4-2 on page 88. The last device of that SCSI chain must have a valid terminator. The SCSI ID set-up button is located at the rear of the IBM 3580.

[2] All media and cleaning cartridges are warranted separately from the IBM 3580 Ultrium tape drive.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1477
Doc: 3690

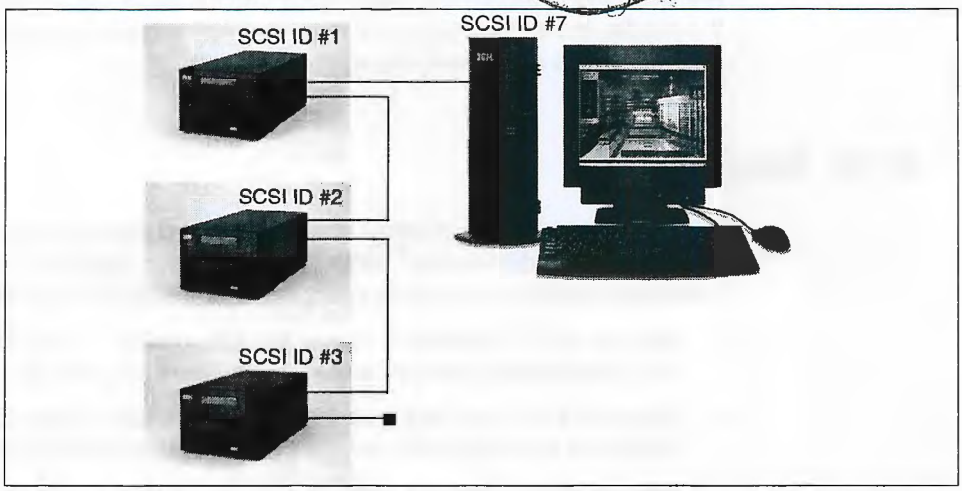


Figure 4-2 SCSI ID set-up example

4.12 Operator displays and buttons

The IBM 3580 Ultrium tape drive has a simple operating interface consisting of:

- A status light
- A message display
- A single character display
- A push button

4.12.1 Status light

The status light (labeled 2 in Figure 4-3 on page 90) provides information about the state of the IBM 3580 tape drive. The light can be green or amber, and, when lit, solid or flashing. These are the possible conditions of the status light and an explanation of what each condition means:

- Off: The IBM 3580 tape drive has no power, or is powered off, or if C displays simultaneously in the single-character display (see label 3 in Figure 4-3 on page 90), it needs cleaning.
- Green/solid: The IBM 3580 tape drive is idle.
- Green/flashing: The IBM 3580 tape drive is reading or writing data, rewinding the tape, locating data on the tape, or unloading the tape.
- Yellow/solid: The IBM 3580 tape drive is in maintenance mode, or is running power-on self-test diagnostic routines.

- Yellow/flashing: One of the following applies:
  - If the light flashes once per second, an error occurred and the tape drive or media may require service. Note the code on the single-character display. Refer to the Setup and Operator Guides (GA32-0415 for Ultrium1 or GA32-0460 for Ultrium 2).
  - If the light flashes twice per second, the tape drive is updating firmware.
  - If the light flashes four times per second, the tape drive detected an error and is performing a firmware recovery. It resets automatically.

4.12.2 Message display

The message display (labeled 4 in Figure 4-3 on page 90) is a liquid crystal display (LCD) that provides information about the status of the tape drive and error conditions.

The message display consists of two rows, with 20 characters available in each row. During operation, the IBM 3580 tape drive continuously queries the drive and updates the display with status messages. When in an idle (non-operating) state, the tape drive displays the following messages:

```
Ultrium Tape Drive
Drive Empty
```

4.12.3 The single-character display

The IBM 3580 tape drive features a light-emitting diode (LED) display (labeled 3 in Figure 4-3 on page 90 below). The LED presents a single-character code for:

- Error conditions and informational messages
- Diagnostic or maintenance functions (while in maintenance mode only)

For the list of messages, refer to the Setup and Operator Guides (GA32-0415 for Ultrium1 or GA32-0460 for Ultrium 2).

If multiple errors occur, the code with the highest priority (represented by the lowest number) displays first. When the error is corrected, the code with the next highest priority displays, and so on, until no errors remain.

The single-character display is blank during normal operation of the IBM 3580 tape drive.

ROS nº 03 2005 - CN
CPMI - CORREIO
Fls. Nº 1478
Doc: 3690

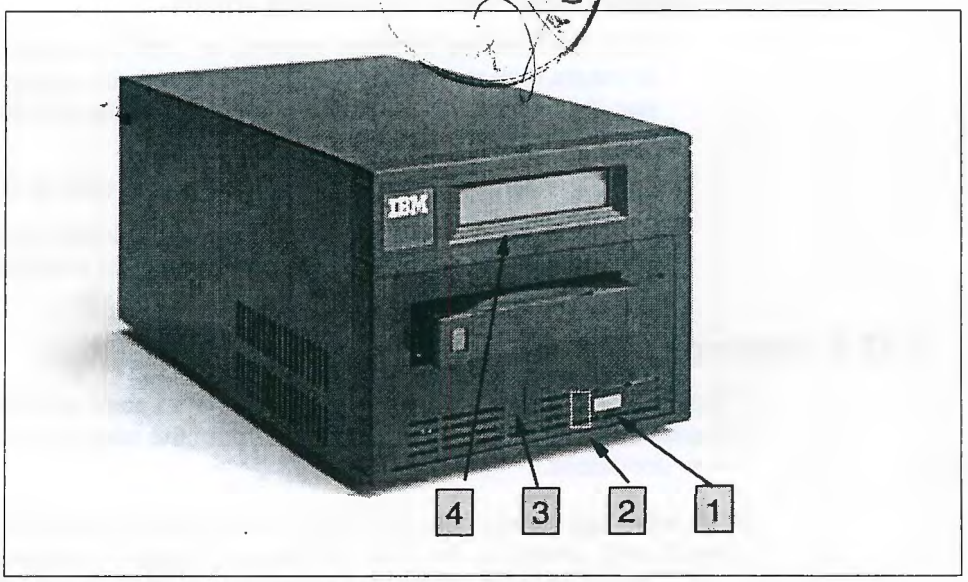


Figure 4-3 Front view of the IBM 3580 tape drive

4.12.4 Unload push button

The unload push button (labeled 1 in Figure 4-3) enables you to perform several functions. You can:

- Rewind the tape from the cartridge and eject the cartridge from the tape drive.
- Place the tape drive in maintenance mode
- Scroll through the maintenance menus
- Exit from the maintenance mode.

Attention: If you press the Unload button during operation, the IBM 3580 tape drive ends the current job, and unloads and ejects the tape cartridge.

4.13 Drive cleaning

All IBM Ultrium tape drives have an integrated cleaning mechanism that brushes the head at cartridge load time and again when unloading a cartridge. Along with this, the drives have a cleaning procedure that uses a special cleaning cartridge.

To clean the head, insert the cleaning cartridge into the tape load compartment. The tape drive performs the cleaning operation automatically. When the cleaning operation is finished, the drive ejects the cartridge.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

The IBM 3580 needs cleaning when the IBM 3580 tape drive status light (label 2 in Figure 4-3 on page 90) is OFF and C displays simultaneously in the single-character display (label 3 in Figure 4-3 on page 90). This is the only occasion when a cleaning cartridge should be used. For normal operation, the integrated cleaning mechanism ensures that the head remains clean.

4.14 Firmware upgrade

Each IBM Ultrium Tape drive contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the latest firmware level is installed on your IBM LTO tape drive. As the IBM 3580 is designated as a Customer Setup Machine, it is the customer's responsibility to have current firmware installed.

Determine the latest level of firmware available from the Web site:

`http://www-1.ibm.com/support/docview.wss?rs=543&org=ssg&doc=S4000055&loc=en-us`

Follow the instructions for updating your firmware in the Setup and Operator Guides (GA32-0415 for Ultrium1 or GA32-0460 for Ultrium 2) or from:

`http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_drivefw`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1479
3690
Doc:

5

IBM TotalStorage Ultrium Tape Autoloader 3581

The IBM TotalStorage Ultrium Tape Autoloader 3581 (see Figure 5-1 on page 95) is the second product in the IBM LTO Ultrium family. It is an external, single-drive, SCSI-attached, stand-alone or rack-mounted autoloader that attaches to iSeries, AS/400, pSeries, RS/6000, RS/6000 SP, xSeries, Netfinity®,Microsoft Windows NT, Microsoft Windows 2000, Windows 2003, Sun Solaris, HP-UX, and Linux systems using a SCSI adapter.

The IBM TotalStorage Ultrium Tape Autoloader 3581 uses a single IBM LTO Ultrium tape drive. The autoloader contains seven tape slots[1] providing a media capacity of up to 700 GB (1.4 TB with 2:1 compression) per autoloader, and is capable of sustaining a data rate of up to 15 MBps (uncompressed).

The IBM TotalStorage Ultrium Tape Autoloader 3581 is an excellent solution for customers who use tape and require a larger capacity or higher performance tape backup, with or without random access, than is provided by their current tape system. With its higher capacity and performance, the 3581 is an excellent replacement for other externally attached DLT, SDLT, 1/4-inch, 4 mm, or 8 mm tape devices for the iSeries, AS/400, pSeries, RS/6000, RS/6000 SP, xSeries, and Netfinity families of workstations and servers.

[1] When the optional barcode reader is installed the cartridge capacity is reduced to six.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1480
Doc: 3690

For capacity and performance requirements beyond a single IBM Ultrium drive and seven IBM Ultrium tape cartridges, consider other solutions in the IBM Ultrium familysuch as the IBM TotalStorage Tape Library 3582, IBM TotalStorage Ultrium Scalable Tape Library 3583, or IBM TotalStorage UltraScalable Tape Library 3584.

5.1 Model description

The IBM TotalStorage Ultrium Tape Autoloader 3581 is a high-performance Ultrium tape autoloader. It is available as four separate model types, depending on the capacity and required SCSI[2] interface.

Figure 5-1 IBM TotalStorage Ultrium Tape Autoloader 3581

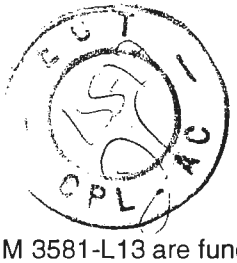
The four models are:

- *IBM 3581-L17* and *IBM 3581-L13* have seven cartridge slots, a .7 TB native data capacity with a Low-Voltage Differential (LVD) Ultra2 SCSI attachment that connects to LVD fast/wide adapters.
- *IBM 3581-H17* and *IBM 3581-L13* have seven cartridge slots, a .7 TB native data capacity with a High-Voltage Differential (HVD) Ultra SCSI attachment that connects to HVD fast/wide adapters.

The IBM 3581-L17, -L13, -H17, and -H13 all use the same Ultrium 1 LTO cartridge, which has a capacity of 100GB (200GB with 2:1 compression), and are capable of sustaining a data rate of up to 15 MB/s (uncompressed).

[2] Refer to2.4.3, "Interfaces" on page 31 for an explanation of HVD and LVD.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1481
Doc: 3690



The IBM 3581-L17 and IBM 3581-L13 are functionally identical, as are the IBM 3581-H17 and IBM 3581-H13. The only difference is that the IBM 3581-L13 and the IBM 3581-H13 have a three-year Customer Element Exchange warranty.

Note: Although the IBM TotalStorage Ultrium Tape Autoloader 3581 provides the capability for high tape performance, other components of the system may limit the actual performance achieved. Also, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

5.1.1 Feature codes

The IBM 3581 can be ordered and/or upgraded with the following feature codes (Table 5-1). We have not included the various cabling options; refer to the product publications for detailed information about configuring and ordering the IBM TotalStorage Ultrium Tape Autoloader 3581.

Table 5-1 IBM 3581 feature codes

Feature Code	Description	Comments
1748	Custom QuickShip	
7003	5U rack mount option	Plant or field install
7004	Barcode reader	
8001	One 100GB data cartridge	Plant only, see Media section for details.
8002	One cleaning cartridge	Plant only, see Media section for details.
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9400	Attached to AS/400	
9600	Attached to AIX	

5.1.2 Access mode

The IBM 3581 can be operated in sequential or random-access modes. In sequential mode, the IBM 3581 loads cartridges one after another, controlled by

the hardware when it receives the unload command from the host server. In random-access mode, the IBM 3581 relies on application software for cartridge management.

5.1.3 SCSI devices

Although it has only a single tape drive, the 3581 appears as two SCSI devices on the SCSI bus. In other words, the autoloader and the drive have separate SCSI addresses.

The IBM 3581 only operates on a single path, and control of the autoloader is handled by a single server. Connection to multiple servers can be achieved when using SAN technology and appropriate application software for cartridge management, such as IBM Tivoli Storage Manager V3.7 or higher.

5.1.4 Adding and removing cartridges

The IBM 3581 does not have a cartridge I/O station. In order to insert and remove cartridges from the slots you have to open the autoloader door. The IBM TotalStorage Ultrium Tape Autoloader 3581 can contain up to seven tape cartridges:

- Five cartridges in the front, slots 1 through 5
  (referred to as front slots; see label 1 in Figure 5-2)
- Two cartridges in the rear, slots 6 and 7
  (referred to as rear slots; see label 2 in Figure 5-2)

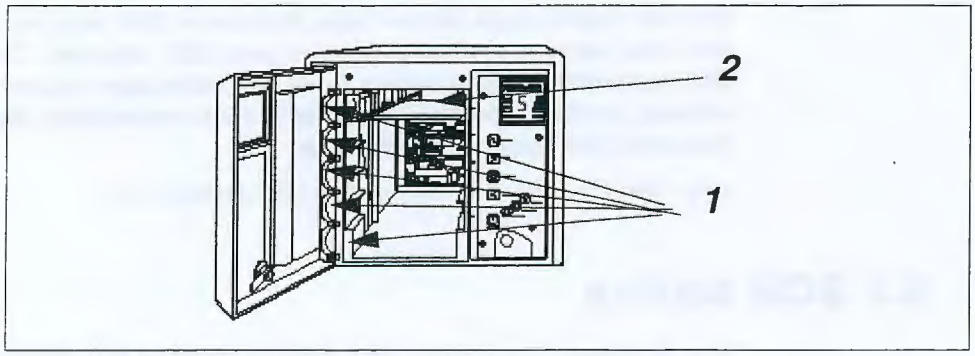


Figure 5-2 IBM 3581 cartridge slots

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1482
Doc: 3690

5.1.5 Operation

The IBM 3581 autoloader is designed for easy, unattended operation. An optional barcode reader makes tape inventory tasks more efficient. Indicators on the operator's panel provide information about:

- Power
- Autoloader and drive activity
- Error status
- Message information

Push buttons provide display, mode, and power controls.

5.2 SCSI attachments

The SCSI interface (HVD or LVD) on each IBM TotalStorage Ultrium Tape Autoloader 3581 is chosen by selecting the appropriate model number (H17/13 or L17/13).

The IBM TotalStorage Ultrium Tape Autoloader 3581 can be attached to iSeries, AS/400, pSeries, RS/6000, xSeries, Netfinity, HP, Sun, UNIX, and PC servers that support Ultra/Wide SCSI HVD and Ultra2/Wide SCSI LVD interface specifications. The interface you choose will depend on the available adapter in the host, which must be of the same type as the drive interface.

SCSI cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code should also be specified.

The IBM TotalStorage Ultrium Tape Autoloader 3581 also may be compatible with other servers, operating systems, and SCSI adapters. Contact your local IBM representative for a current list of supported open system configuration and software vendors. You also may refer to the Interoperability Matrix (List of Supported Servers) on this Web site:

`http://www.storage.ibm.com/tape/lto/3581/3581opn.pdf`

5.3 SCSI cabling

A SCSI cable is required for each 3581 connection to a SCSI bus. A single 2.5 m SCSI cable is available as a no-charge feature; if an alternate length is required it should be included in the initial order. A SCSI terminator is included with each autoloader. An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) also may be required for attachment to particular server adapters.

5.3.1 Cables

A single SCSI cable is available as no-charge feature #9702 or #9703 only with the initial IBM 3581 order. These no-charge features cannot be ordered later as a miscellaneous equipment specification (MES); however, the same cables can be ordered later as chargeable MES upgrades using feature codes #5302 and #5602. Feature #9702 supplies a 2.5 m SCSI cable with HD68 connectors at each end; feature #9703 differs in that one end has a VHDCI connector.

Additional SCSI cables are available as optional features on the IBM 3581 for LVD and HVD attachment to host adapters:

- Feature #5301, 0.4 m (1.4 feet) SCSI cable
- Feature #5302, 2.5 m (8.2 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The cables can be used with an HVD Ultra SCSI bus or LVD Ultra2 SCSI bus and have an HD68 connector on each end. A SCSI terminator is included with each Ultrium autoloader.

The following cables differ in that they have a VHDCI connector at one end:

- Feature #5602, 2.5 m (8.2 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 2 5m (82 feet) SCSI cable

5.3.2 Interposers

An interposer is required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries adapter #6501.
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable.

  This interposer (a 0.3 m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

RQ/TP 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1483
Doc: 3690

5.3.3 SCSI length limitations

The IBM 3581 has one SCSI ID for the drive and one for the loader, so the SCSI interconnection is multi-drop. This means that the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

5.4 Upgrades and optional features

The IBM 3581 H17/13 and L17/13 are single tape drive autoloaders and cannot be upgraded to any other models.

Two additional optional features are available:

- Feature #7003, 5U Rack Mount Option
  The IBM 3581 can be installed as a stand-alone single unit, or two units can be mounted side-by-side in a standard 19-inch rack, requiring 5 EIA units of rack space. This chargeable feature provides the necessary hardware to mount the autoloader in the rack.
- Feature #7004, Barcode Reader
  This optional chargeable feature enables the IBM 3581 autoloader to read cartridge information contained in a barcode label on the IBM Ultrium cartridges. User-installed application software provides the inventory management functions enabled by the barcode reader feature.

  Note: Installing feature #7004 reduces the autoloader capacity to six data cartridges. The barcode reader connects to the interface connector on the inside top panel of the IBM 3581. This location prevents you from using cartridge storage slot 1 (see Figure 5-2 on page 97). When you install the barcode reader, you reduce the capacity of the autoloader to six cartridge storage slots. The front storage slots are still numbered 1 through 5, but the autoloader's menu functions and the server's application software cannot select or use slot 1.

  This is illustrated by observing that, with the barcode reader installed, the operator LOAD SLOT function uses storage slots 2 and 3 as the cartridge source locations to load slots 6 and 7; without the barcode reader installed, the LOAD SLOT function uses storage slots 1 and 2 as the source locations. See Figure 5-2 on page 97 for slot locations.

5.5 Environmental specifications

The IBM 3581 is a medium-sized desktop or stand-alone unit that optionally can be integrated into a standard 19" rack for space optimization. Two IBM 3581s can be installed side-by-side in a rack using 5 EIA space units.

5.5.1 Physical dimensions

The IBM 3581 models H17/13 and L17/13 are medium-sized single tape drive autoloaders:

- Width: 21.9 cm (8.62 in)
- Depth: 58.1 cm (22.87 in)
- Height: 19.0 cm (7.48 in)
- Maximum weight: 13.0 kg (28.7 lbs)

5.5.2 Operating environment

The IBM 3581 can be installed in a normal office environment and does not need to be in a specialized machine room.

5.6 Host platforms and device drivers

The following no-charge specify codes indicate the server platform to which the IBM 3581 is attached.

- #9210, attached to HP-UX
- #9211, attached to Sun system
- #9212, attached to Windows NT system
- #9213, attached to other non-IBM system
- #9400, attached to iSeries system
- #9600, attached to RS/6000 system

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3581). Sometimes the driver code is supplied as part of the operating system code (such as, in OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1484
Doc: 3690

Ultrium 1

The IBM TotalStorage Ultrium Tape Autoloader is shipped with device drivers to support Ultrium 1 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.2 or later
- Sun Solaris 2.6, 7, and 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- Windows 2003
- HP-UX 11.0
- OS/400 V4R4

Tip: The device driver CD or diskette that is shipped with the IBM 3581 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Therefore you should always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

5.6.1 Device driver installation

Install the IBM device drivers for the IBM 3581 as follows:

- If you intend to use the IBM 3581 with a storage management application (such as Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3581.
- If you do not intend to use the IBM 3581 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the autoloader. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide,* GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3581 with a commercial software application, IBM recommends that you install an IBM-supplied device driver *only* if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, conflicts could occur over which driver controls the tape subsystem. Many examples of using the Ultrium drives are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

5.7 Storage applications

The software to manage the IBM 3581 is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software vendors. A list of compatible software is available at:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1 and Ultrium 2 support and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more-detailed information of specific versions and platforms supported.

5.8 Performance considerations

For best performance, it is recommended to attach only one tape drive per SCSI bus. This may not be a realistic objective, but minimizing the number of devices per bus will improve performance. Attaching other SCSI devices on the same SCSI bus as the IBM 3581 drive may affect performance of those devices.

iSeries configurators allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape drive on an input/output port may affect system performance.

Although the compression technology can increase the amount of data stored on the media, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

5.9 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each autoloader order[3]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3581:

- Feature #8001 provides a single 100 MB Ultrium Data Cartridge.
  It is a chargeable feature, and a maximum of seven can be ordered.
- Feature #8002, provides a single Ultrium Cleaning Cartridge.
  It is a chargeable feature, and a maximum of three can be ordered.

[3] All media and cleaning cartridges are warranted separately from the IBM TotalStorage Ultrium Tape Autoloader 3581.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1485
Doc: 3690

Subsequent to the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about ordering supplies and cartridges, with or without labels.

5.10 IBM 3581 initial setup

The following section covers some of the major items required to implement, manage, and operate the IBM 3581 tape library. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the Setup and Operator Guide and to the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

5.10.1 SCSI ID

The IBM 3581 consists of two SCSI devices: the autoloader and the drive. The default settings for the SCSI IDs as displayed on the message display panel are LdR Id 1[4] (for the autoloader) and dRV Id 3 (for the drive). Depending on your requirements, you may need to change the SCSI ID default settings for your installation. When setting a SCSI ID:

- Do not select an ID that is already in use.
- Do not select the SCSI ID of the server SCSI adapter card. The SCSI ID of the server SCSI adapter card is usually higher than any device on the SCSI bus. Generally, the SCSI ID for the server adapter is set to 7.
- Do not use F, as it is reserved for internal use by the SCSI library.
- Unless you choose another operation, the IBM 3581 times out 30 seconds after each operation and LdR REAdY appears in the message display (label 1 in Figure 5-3 on page 106).
- Functions and messages in the message display can only be scrolled forward. To select a previously viewed function, continue to scroll through the choices until the function that you want appears on the message display.
- As with the IBM 3580, the IBM 3581 can be part of a SCSI chain. The same rules apply for SCSI addresses as for the IBM 3580.

Refer to the Setup and Operator Guide for details about determining and changing the SCSI IDs.

[4] The message display panel displays a D as a lower case letter so we have shown the message as it would appear.

5.10.2 Element numbers

Element numbers (also called element addresses) identify the physical location within the autoloader. This information is required by storage management applications such as the Tivoli Storage Manager.

The three types of elements in the IBM 3581 are shown in Table 5-2:

Table 5-2 IBM 3581 element numbers

Element	Element number
Picker (media transport element)	57 hexadecimal
Tape drive (data transfer element)	52 hexadecimal
Storage element	01 - 07 hexadecimal

The IBM 3581 has one storage element for each of the cartridge storage slots.

A host application controls movement within the autoloader by issuing one of these SCSI commands:

- MOVE MEDIUM

  This SCSI command tells the autoloader to move a cartridge from the source element to the destination element. The elements are identified using the element numbers shown in Table 5-2. So, for example, a MOVE MEDIUM command could be issued to tell the library to move a cartridge from the picker to the drive.

- POSITION TO ELEMENT

  This SCSI command positions the picker to a specified element number.

5.10.3 Operator displays and buttons

Management of the IBM 3581 is performed by using the status lights, message display panel, and push buttons on the control panel behind the front door.

Status lights

The IBM TotalStorage Ultrium Tape Autoloader 3581 features three status lights on the operator panel (label 2 in Figure 5-3 on page 106):

- POWER: The green POWER light comes on whenever you turn on the power.
- ACTIVITY: The amber ACTIVITY light indicates robotic or drive activity. A slowly blinking light indicates robotic activity; a rapidly blinking light indicates drive activity.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1486
Fls. Nº
3690
Doc:

- ALARM: The red ALARM light comes on whenever an error occurs. To resolve the error refer to the Setup and Operator Guide.

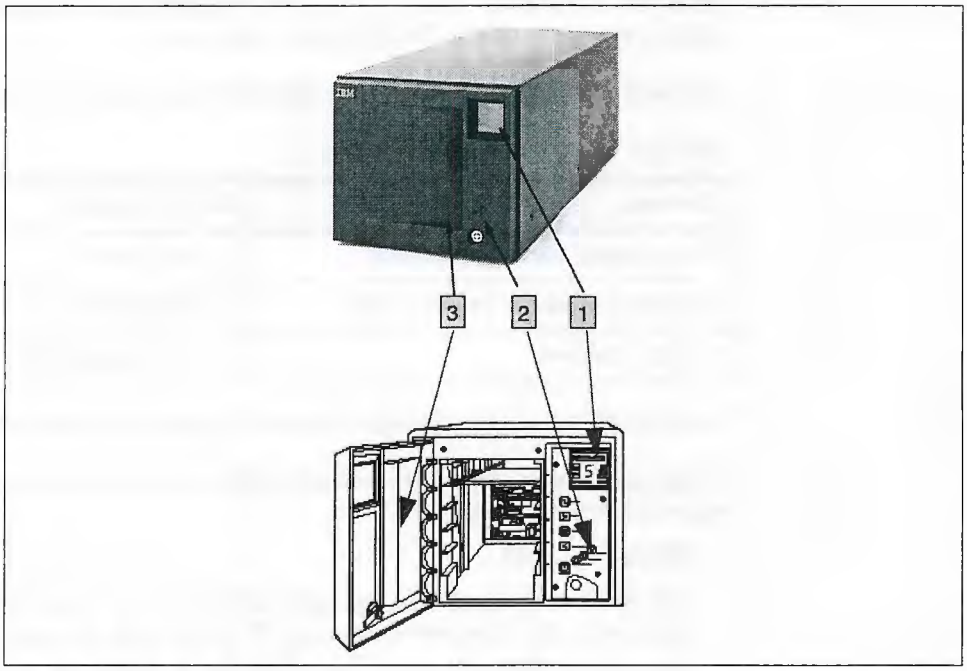


Figure 5-3 IBM 3581 front view

5.10.4 Message display

The IBM TotalStorage Ultrium Tape Autoloader 3581 offers a one-line, 10-character front panel with a liquid crystal display (LCD) that provides operational information as well as diagnostics and messages.

The LCD message display (label 1 in Figure 5-3) provides information about the status of the IBM TotalStorage Ultrium Tape Autoloader 3581 and any error conditions. When in an idle (non-operating) state, the autoloader message panel displays LdR REAdY. In addition, the following characters (shown in Figure 5-4 on page 107) may appear on the left side of the display:

- DC: Indicates that data compression is selected on the drive.
- WP: Indicates that a write-protected data cartridge is loaded in the drive.
- CT: Indicates that the drive head needs to be cleaned.

The large field in the center of the display indicates the number of the storage slot from which the picker removed a cartridge for loading into the drive.

Whenever an error occurs, E displays in this field and the error message is displayed on line 1.

The activity bars on the right (in conjunction with the activity light) indicate robotic and drive activity:

- The bottom bar blinks when no activity is taking place.
- A slow interval between the bars appearing and disappearing indicates robotic activity.
- A fast interval between the bars appearing and disappearing indicates drive activity.

The seven numeric fields at the bottom of the display indicate the current cartridge inventory. Each will appear only if a cartridge is present in that storage slot, as shown in Figure 5-4.

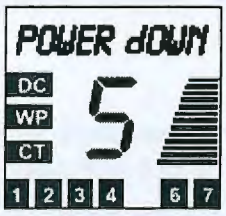


Figure 5-4 IBM 3581 message display

5.10.5 Drive status messages

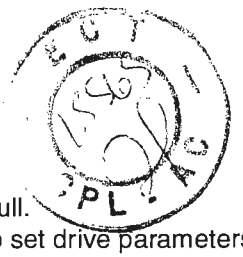
During operation, the IBM 3581 places messages about the drive's status in the message display. These messages can appear:

- CLEANING: The drive is cleaning the head with the cleaning cartridge.
- EJECTING: The drive is unloading the tape.
- ERASING: The drive is erasing the tape.
- LOADING: The drive is loading the tape.
- LOCATING: The drive is locating the position on the tape.
- READING: The drive is reading from the tape.
- REWINDING: The drive is rewinding the tape.
- WRITING: The drive is writing to the tape.

If an error occurs during operation, the IBM 3581 halts the current operation and displays an error code in the message display. The following list provides the most common errors codes and gives a description of each:

- CT FAILED: Cleaning tape failed to clean drive.
- DEST FULL: The destination location was full.
- DRIVE BUSY: The drive is busy and cannot unload the tape.

ROS nº 03.2005 - C
CPMI - CORREI
Fls: Nº 1487
Doc: 3690



- DRIVE FULL: The drive was full.
- DRIVE PGRM: The attempt to set drive parameters failed.
- DRIVE POST: The drive failed its Power-On Self Test (POST).
- FRONT SLOT: A front slot sensor was not tripped.
- FRONT TAPE: A front tape sensor was not tripped.
- LDR INIT: The autoloader could not complete its initialization.
- PCKR EMPTY: The picker was empty.
- PCKR FULL: The picker was full.
- REAR SLOT: A rear slot sensor was not tripped.
- REAR TAPE: A rear tape sensor was not tripped.
- ROBOT POST: The robotics failed its Power-On Self Test (POST).
- SRC EMPTY: The source location was empty.
- SLOT EMPTY: No slot beam was detected.
- PWR SWITCH: The front power switch was pressed.
- SLOT FULL: A cartridge was already in the slot.

This list is not complete. See the Setup and Operator Guide for the full error list.

5.10.6 Control buttons

The control buttons are push buttons on the operator panel that let you interact with the menus on the message display (Figure 5-5 on page 109):

MODE:	Scrolls through the commands that you can use to operate the IBM 3581 (label 1 in Figure 5-5 on page 109).
NEXT:	Highlights the next item or value in the currently displayed menu (label 2 in Figure 5-5 on page 109)
SELECT:	Selects the currently displayed operation (label 3 in Figure 5-5 on page 109).
PREVIOUS:	Highlights the previous item or value in the currently displayed menu (label 4 in Figure 5-5 on page 109).

To operate a button, press and release it. You can use the control buttons to:

- Load a tape cartridge into a drive (LOAd dRV)
- Eject a tape cartridge from the drive and put it into the storage slot that it was loaded from (EJECT dRV)
- Load slot 6 from slot 1, or load slot 7 from slot 2 (LOAD SLOT)
- Move a cartridge from slot 6 to slot 1 or from slot 7 to slot 2 (EJECT SLOT)
- Eject a tape cartridge that was left in the media picker into an empty destination slot (EJECT PCKR)
- Set the SCSI ID of the autoloader or the drive (SET SCSI)

Note: The procedure for loading slots 1 through 5 differs from loading slots 6 and 7. If you are loading seven cartridges, load slots 6 and 7 first. See "Inserting a Cartridge into Slots 6 and 7" of the chapter "Operating the IBM 3581 Tape Autoloader" in the Setup and Operator Guide, which also contains a complete list of commands.

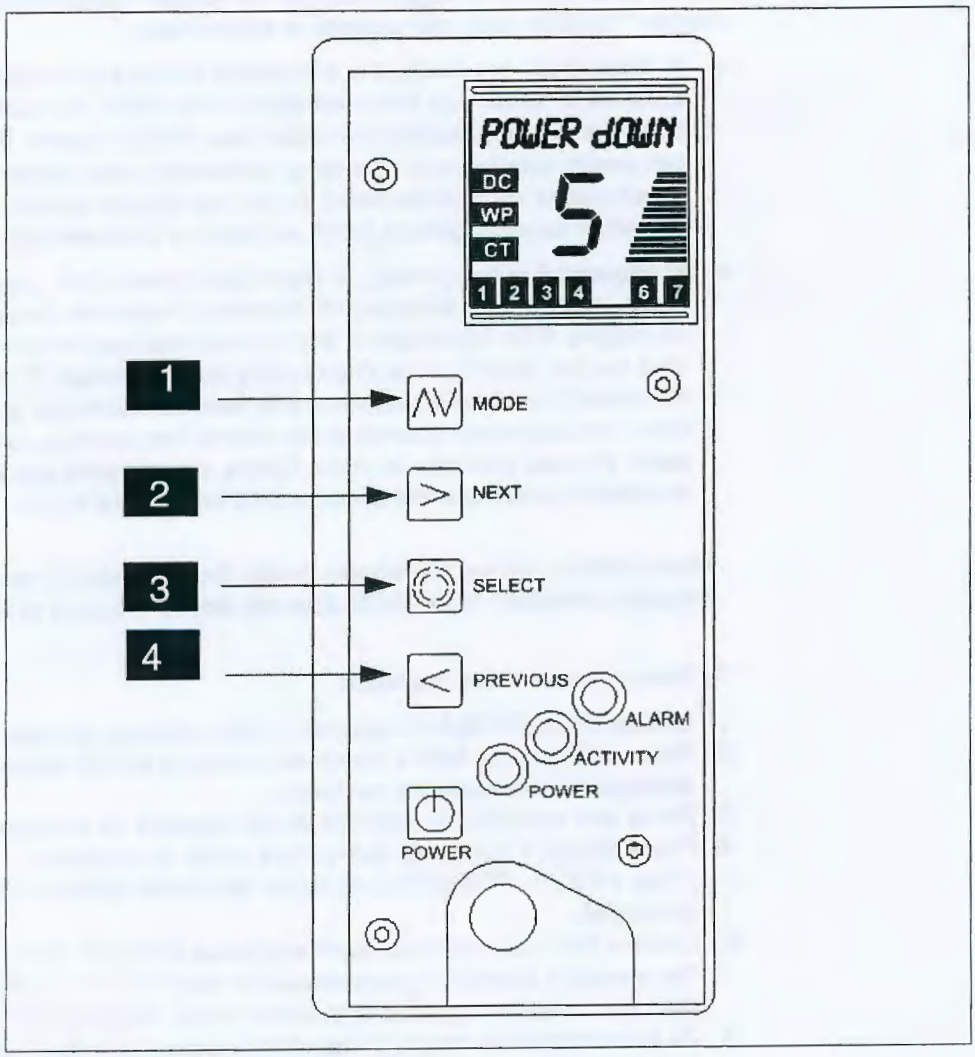


Figure 5-5 IBM 3581 operator panel

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1488
Doc: 3690

5.10.7 Operating modes

The IBM 3581 operates in both random access mode (in which the server's application software manages the cartridges) and sequential access mode (in which the autoloader's firmware manages the cartridges).

Change between random and sequential mode through the *Diagnostic Menus*.

Select CHG MODE to toggle between the random access and sequential access modes. The IBM 3581 can operate in either mode:

- In random access mode, the autoloader allows the server's application software to select any data cartridge in any order. You can logically divide cartridge usage to satisfy particular data storage needs. For example, you can assign one or more cartridges to specific data functions (such as certain directories or network servers), or you can assign specific cartridges to individual users or groups (such as Sales or Engineering).
- In sequential access mode, all cartridges present are considered to be a single volume. The autoloader's firmware predefines the selection of the cartridges. After initialization, the firmware causes the autoloader to always load the first cartridge found (counting from 1 through 7) into the drive. After the server's application software has filled this cartridge and unloaded the drive, the autoloader automatically returns the cartridge to its storage slot and loads the next cartridge in order. Empty storage slots are ignored. The autoloader continues this process until the volume is full.

Note: While in sequential access mode, the autoloader's robotics are not logically connected to the SCSI bus and do not respond to SCSI commands.

To change the mode of operation:

1. Ensure that LdR REAdY appears on the message display.
2. Press and hold the NEXT button and then the MODE button until dIAG MENU displays (approximately 5 seconds).
3. Press and hold MODE until CH MOdE appears on the message display.
4. Press SELECT to display the current mode of operation.
5. Press NEXT or PREVIOUS to toggle the mode between SEQUENTIAL and RANdOM.
6. Choose the mode that you want and press SELECT. CYCLE PWR blinks on the message display. If you changed to random mode, LdR REAdY then displays; if you changed to sequential mode, SEQ REAdY then displays.
7. To activate the new mode of operation, cycle power (turn off, then on) to the IBM 3581.

The complete list of mode set-up commands is in the Operator and Setup Guide.

5.11 Drive cleaning

All IBM Ultrium tape drives have an integrated cleaning mechanism that brushes the head at load time and again when unloading a cartridge. There is also a cleaning procedure using a special cleaning cartridge.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

The IBM 3581 internal tape drive determines when the head needs to be cleaned and alerts you by displaying CT on the message display (label 1 in Figure 5-3 on page 106). This is the *only* occasion when a cleaning cartridge should be used. The IBM 3581 supports three methods of cleaning the drive:

- Host cleaning
  Host cleaning enables the server software to detect the need to clean an Ultrium Tape Drive and to control the cleaning process. The cleaning cartridge must be stored in one of the available storage slots within the 3581.
- Automatic cleaning (AUTOCLEAN)
  Automatic cleaning enables the 3581 to automatically respond to any tape drive's request for cleaning and to begin the cleaning process. Automatic cleaning makes the cleaning process transparent to any host application using the autoloader. If the server application does not support the host cleaning function, use the autoclean function.
- Manual cleaning
  Manual cleaning requires you to select a menu option from the autoloader's display. Manual cleaning is always supported, regardless of whether host cleaning or automatic cleaning is enabled or disabled.

In all methods, the autoloader performs the cleaning after you unload the data cartridge from the drive and before the next load.

Note: Whenever you enable host application cleaning or the autoloader's autoclean function, the tape capacity of the autoloader is reduced to six tapes without the barcode reader and to five cartridges with the barcode reader feature installed. The extra slot is used for storing the cleaning cartridge within the IBM 3581.

Proper instructions for cleaning the IBM 3581 tape drive can be found in "Performing Diagnostic and Maintenance Functions" in the Setup and Operator Guide.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1489
Doc: 3690

5.12 Firmware upgrade

Each IBM Ultrium Tape drive and library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the latest firmware is installed on your IBM LTO Autoloader. As the IBM 3581 is designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed.

Determine the latest level of firmware available from the Web site:

```
http://www-1.ibm.com/support/docview.wss?rs=541&context=STCVQ6N&q=ssg1*&uid=ssg
1S4000042&loc=en_US&cs=utf-8&lang=en+en
```

Follow the instructions for updating your firmware in the *IBM 3581 Ultrium Tape Autoloader Setup, Operator, and Service Guide*, GA32-0412, or from:

```
http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_dri
vefw
```

1556

6

IBM TotalStorage Ultrium Tape Library 3582

The newest member of the IBM Ultrium family is the IBM TotalStorage Ultrium Tape Library 3582, shown in Figure 6-1 on page 114. It is a high-performance, reliable, scalable tape subsystem. Designed for tape automation, the IBM TotalStorage Ultrium Tape Library 3582 (IBM 3582) can be attached to iSeries, pSeries, xseries, Intel (running Windows or Linux), Sun SPARC, Hewlett-Packard, and other open systems using SCSI or Fibre Channel attachment. It uses IBM Ultrium 2 tape drives for faster data transfer and reliability in automated library service. Each aspect of the library subsystem has been optimized for repeated, reliable unattended tape handling.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1490
Doc: 3690

6.1 Model description

The IBM 3582 tape library houses one or two IBM Ultrium 2 tape drives, which each have a native data transfer rate of 35 MBps and a cartridge capacity of 200 GB. The drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm that provides an effective data rate of up to 70 MBps and a cartridge capacity of up to 400 GB (with 2:1 compression) on IBM Ultrium 2 media. Multiple drive models provide additional enhanced functions such as faster transfer of data, simultaneous backup, concurrent read-write operations, and fault tolerance through Control Path Failover.

The IBM 3582 has one I/O slot plus additional cartridge capacity of 23 slots (24 slots in all), allowing a native capacity of 4.8 TB of uncompressed data. With compression (assuming 2:1), the IBM 3582 can store 9.6 TB of data. These capacities assume that the I/O slot has been configured as an additional storage slot, increasing the overall library capacity.

The IBM 3582 is an excellent high-performance, entry-level choice for entry-level and midrange systems.

Figure 6-1 IBM TotalStorage Ultrium Tape Library 3582

The IBM TotalStorage Ultrium Tape Library 3582 supports three Ultrium 2 drive types: Ultrium 2 LVD, Ultrium 2 HVD, and Ultrium 2 FC. The drives can be intermixed. The IBM 3582 comes standard with multi-path architecture and the ability to partition the library into two logical libraries. The library can be configured as a stand-alone unit or mounted in an industry-standard 19-inch

rack. Additional optional features include Control Path Failover for AIX and a Remote Management Unit/Specialist for remote library management.

Table 6-1 IBM 3582 model summary

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	IBM Ultrium tape drives
3582-L23	23[a]	4.4 TB	8.8 TB	1-2

a. Plus one I/O Station slot that can be assigned as a storage slot. If this is done, the library capacity is 4.8 TB (9.6 TB compressed).

6.1.1 Tape drives

The IBM 3582 libraries use IBM LTO Ultrium 2 tape drives. It is mandatory to have at least one IBM Ultrium drive installed in the library. An additional drive may be added at the initial order or as a field upgrade performed by the customer.

The installed drives may be any mixture of LVD, HVD, or FC. The drives are ordered for plant or field installation using chargeable feature codes:

- Feature #8103 provides one IBM Ultrium 2 tape drive with a Low Voltage Differential (LVD) Ultra2/Wide SCSI Connection.
- Feature #8104 provides one IBM Ultrium 2 tape drive with a High Voltage Differential (HVD) Ultra/Wide SCSI Connection.
- Feature #8105 provides one IBM Ultrium 2 tape drive with a Native 2 Gb Fibre Channel Connection.

Each IBM Ultrium tape drive contains the electronics and logic for reading and writing data, control of the tape drive, management of the data buffer, and error-recovery procedures. All tape drives are packaged as a common assembly that is a Field Replaceable Unit (FRU), designed for quick removal and replacement.

6.1.2 Cartridge storage

As well as the installed tape drives, the library enclosure contains cartridge storage slots, arranged in two rows. The row toward the front of the library is made of two removable magazines of seven slots each. The row toward the rear of the library contains nine slots (Figure 6-3 on page 116). The magazines are designed so that tape cartridges can only be inserted in the proper orientation. Once inserted, the tape cartridges will be retained in the magazine so that they remain in place even when the magazine is inverted and shaken lightly. The magazines can only be inserted one way into the mounting columns in the library.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1491
Doc: 3690

In Figure 6-2, one magazine is loaded and the other is removed.

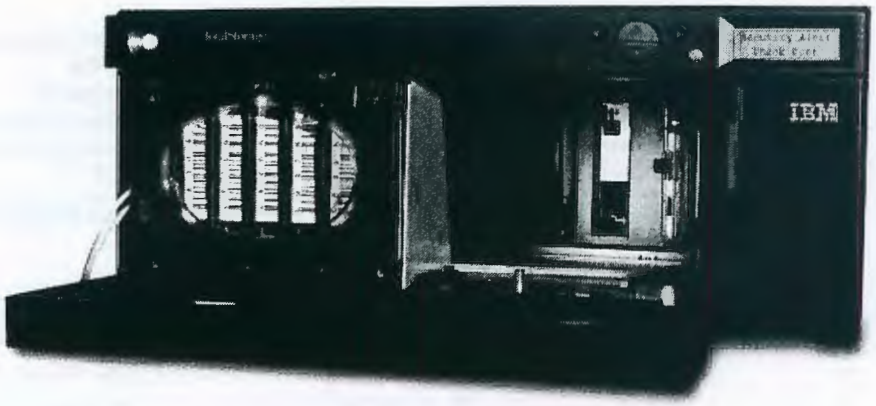


Figure 6-2 IBM 3582 seven-slot magazines

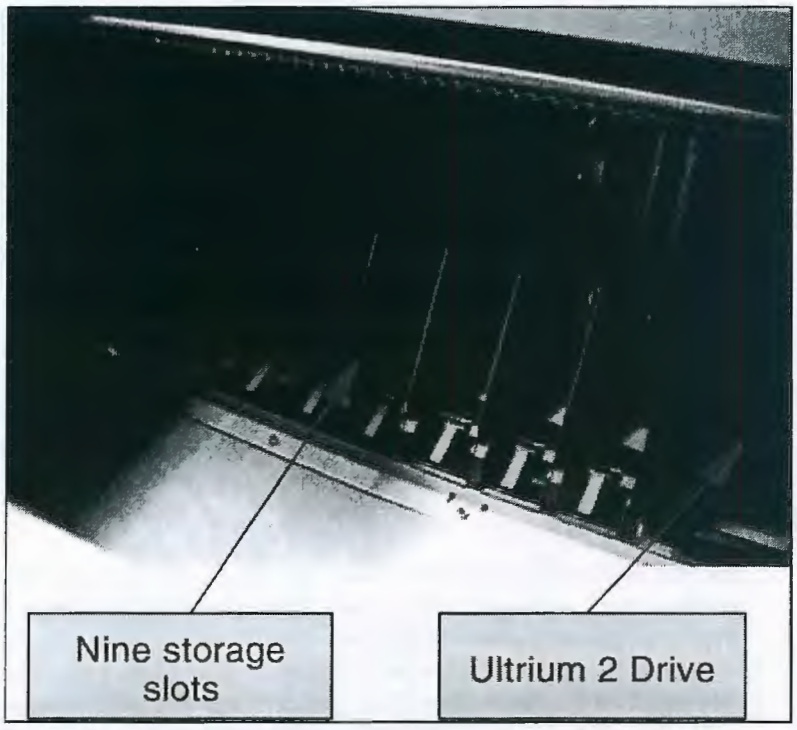


Figure 6-3 IBM 3582 rear-mounted storage slots

6.1.3 Barcode scanner

A barcode scanner is provided as standard with the IBM 3582-L23, and it does not affect the slot capacity of the libraries. The barcode scanner is used during the inventory process to locate all cartridges inserted into the library. This action is repeated every time the front door is opened to ensure that the inventory is updated if a cartridge has been manually added, moved, or removed while the door was open.

6.1.4 I/O station

This facility enables the insertion and ejection of cartridges without interrupting the normal operation of the library. There is a single-slot I/O station where a cartridge can be inserted or ejected by opening the I/O station door.

6.1.5 Robotic system

In conjunction with the library control microcode, the robotic system identifies and moves cartridges between the storage slots, tape drives, and the I/O station. It has a number of components:

- A cartridge picker for placing cartridges in storage slots, tape drives, or the I/O station
- A bar code scanner used to set up the library initially when it identifies the types of storage arrays and tape drives installed in the library, and in normal operation for reading the external labels on the cartridges, when it locates and categorizes all cartridges installed in the library
- X-axis and Z-axis drive motors for moving the picker assembly inside the library enclosure

6.1.6 Library control and operation

The library control unit contains the electronics and logic for autochanger operations. It controls all operations in the IBM 3582 library, including the interaction between the library and operators. The control unit Licensed Internal Code creates and maintains the library configuration, the physical location of the robotic system, and the inventory of cartridges. The database is kept in the flash memory of the library control hardware.

Requests issued from the server result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges to and from the tape drives and for inserting and ejecting cartridges. The host has records of the physical location of a cartridge in the library, and the physical location is also managed by the library.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1492
Doc: 3690

In addition to requesting movement of cartridges in the library, the host can obtain status, performance, configuration information, and information about the cartridges stored in the IBM 3582 tape library.

Each cartridge must have a machine- and operator-readable external barcode label to identify a media cartridge in the library during initial inventory and any time a cartridge is added to the library. The library stores the physical location of the cartridge in an inventory database based on the cartridge label. All host application requests for operations involving movement or use of a cartridge need only reference the physical location of the cartridge (using an element number as described in 6.10.2, "Identifying library location element numbers" on page 125) for the library to perform the request.

6.1.7 Operator panel

An LCD operator control panel on the front of the machine provides status information and menu options. From this panel the operator can initiate actions such as moving and loading tape cartridges or invoking diagnostics.

6.1.8 Maintenance

The cartridge storage slots, cartridge picker, and tape drives are accessed for maintenance purposes by opening the front door of the library. The tape drives, power supplies, and host interface board are reached from the back of the library.

6.2 Feature codes

The IBM 3582 can be ordered and/or upgraded with the feature codes shown in Table 6-2. We have not included the various cabling options; refer to the product publications for detailed information about configuring and ordering.

Table 6-2 IBM 3582 feature codes

Feature	Description	Comment
1660	RMU/Specialist	
1680	Control Path Failover	
2200	Standalone Kit	
7003	Rack Mount Kit	
8101	1 data cartridge	Plant only, see Media section for details.

Feature	Description	Comment
8002	1 cleaning cartridge	Plant only, see section Media for details.
8103	Ultrium 2 LVD drive	
8104	Ultrium 2 HVD drive	
8105	Ultrium 2 Native FC drive	
8203	CSU Ultrium 2 LVD drive	Customer Setup
8204	CSU Ultrium 2 HVD drive	Customer Setup
8205	CSU Ultrium 2 Native FC drive	Customer Setup
8110	20 data cartridges	
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9215	Attached to Linux	
9400	Attached to AS/400	
9600	Attached to AIX	

6.3 Physical attachments

The IBM 3582 tape library can be attached to IBM iSeries, IBM pSeries, IBM RS/6000 and SP systems, IBM xSeries and non-IBM servers, workstations, and personal computers that support the Ultra/Wide SCSI HVD, Ultra2/Wide SCSI LVD, and Fibre Channel interface.

SCSI cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code also should be specified.

The IBM 3582 may be compatible with other servers, operating systems, and SCSI adapters. Contact your local IBM representative for a current list of supported open system configuration and software vendors, or go to:

`http://www.storage.ibm.com/tape/lto/3582/3582opn.pdf`

RQS nº 03/2005 - CN - CPMI - CORREIOS
1493
Fls. Nº
3690
Doc:

6.4 SCSI cabling

A SCSI cable is required for each library connection to a SCSI bus. If no cable is available, one should be specified on the initial order for each library or drive. A SCSI terminator is included with each cable. An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) also may be required for attachment to particular server adapters.

6.4.1 Cables

A host-to-library SCSI cable is available as no-charge feature #9704 or #9705 specified only with the initial IBM 3582 order. One of these cables is supplied with each library ordered. Features #9704 and #9705 cannot be ordered as a miscellaneous equipment specification (MES) for later installation; however, the same cables may be ordered as chargeable MES upgrades after installation by using feature codes #5305 and #5604. Feature #9704 supplies a 4.5 m SCSI cable with an HD68 connector at one end and a VHDCI connector at the other end; feature #9705 supplies a 5 m SCSI cable with HD68 connectors at each end.

Additional SCSI cables are available as optional features on the IBM 3583 for LVD and HVD attachment to host adapters:

- Feature #5302, 2.5 m (8.2 feet) SCSI cable
- Feature #5303, 0.7 m (2.3 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The cables can be used with an HVD Ultra SCSI bus or LVD Ultra2 SCSI bus and have an HD68 connector on each end. A SCSI terminator is included with each Ultrium library.

The following cables differ in that they have a VHDCI connector at one end:

- Feature #5602, 2.5 m (8.2 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 25 m (82 feet) SCSI cable

6.4.2 Interposers

An interposer is required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries to adapter #6501
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable.

  This interposer (a 0.3m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

6.4.3 SCSI length limitations

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection. If using multi-drop interconnection, then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using point-to-point or multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

6.5 Environmental specifications

The IBM TotalStorage Ultrium Tape Library 3582 is a stand-alone, medium-sized library unit that can be placed on a desk or in a rack.

The IBM 3582 has one or two drives and 23 cartridge slots, plus a single-slot I/O station. The physical dimensions are:

- Width: 45.5 cm (17.9 in)
- Depth: 65.4 cm (25.8 in)
- Height: 19.3 cm (7.7 in) for a stand-alone library on casters
- Maximum weight: 30.3 kg (66.7 lb) with two drives
- Four EIA units high (if rack-mounted)

6.6 Host platforms and device drivers

The following no-charge codes indicate the server platform to which the IBM 3582 is attached:

- Feature #9210 attached to HP-UX

Fls. nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1494
Doc: 3690

- Feature #9211, attached to Sun system
- Feature #9212, attached to Windows NT or Windows 2000 system
- Feature #9213, attached to other non-IBM system
- Feature #9215, attached to Linux system
- Feature #9400, attached to iSeries system
- Feature #9600, attached to xSeries

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3582). Sometimes the driver code is supplied as part of the operating system code (such as in OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

The library is shipped with the device drivers to support the following operating environments at the minimal levels shown:

- AIX Versions 4.3.3 or later
- Sun Solaris 2.6, Solaris 7, or 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 (9215)
- Windows 2003
- HP-UX 11.0, 11.i (64 bit)
- OS/400 V5R1 or later
- Linux Red Hat 7.2 (32 and 64 bit kernels), Red Hat 7.3, Red Hat Advanced Server 2.1, SuSE Linux Enterprise Server Update

Tip: The device driver CD or diskette that is shipped with the IBM 3582 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

6.6.1 Device driver installation

Install the IBM device drivers for the IBM 3582 as follows:

- If you intend to use the IBM 3582 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3582.
- If you do not intend to use the IBM 3582 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI*

Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3582 with a commercial software application, IBM recommends that you install any IBM-supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples of using the Ultrium drives are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

6.7 Storage applications

The software for managing the IBM 3582 is not provided with the library. It is not really feasible to use the IBM 3582 without some additional application software to manage the slots and cartridge inventory. Additional software support is available through library management software products, which can be obtained separately from IBM, IBM Business Partners, or independent software providers. A list of compatible software is available at the Web site:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1/2 support and specific Ultrium models and attachment methods. Contact your storage application vendor for more-detailed information about specific versions and platforms supported.

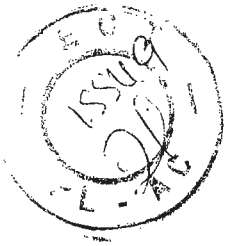
6.8 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each 3582 drive order[1]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3582:

- Feature #8101 provides a single 200 GB Ultrium 2 Data Cartridge. Up to 19 #8101 features can be ordered. The cartridges come with a barcode label but it is not affixed.
- Feature #8002 provides a single Ultrium Cleaning Cartridge. It is a chargeable feature, and a maximum of three can be ordered.
- Feature #8110 provides a pack of twenty 200 GB Ultrium Data Cartridges with un-attached barcode labels.

[1] All media and cleaning cartridges are warranted separately from the IBM 3582.

03/2005 - CN - CPMI - CORREIOS Fls. Nº 1495 Doc: 3690



Subsequent to the initial order, additional supplies may be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about ordering supplies and cartridges, with or without labels.

6.9 Installation and performance considerations

iSeries configurations allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape library on an input/output port may affect drive performance.

Installing more than one Ultrium drive on a SCSI bus may affect tape drive performance. For optimal performance, it is recommended that no more than one IBM Ultrium drive be attached to an individual SCSI bus.

Intermixing of other SCSI devices on the same SCSI bus as the IBM 3582 Ultrium tape library may affect performance of those devices.

While IBM Ultrium tape drives provide the capability for high tape performance, other components of the system may limit the actual performance achieved. The compression technology used in the tape drive can typically double the amount of data that can be stored on the media; however, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

The IBM 3582 Ultrium tape library has multi-path architecture; see 2.6, "Multi-path architecture" on page 46 for more information. This means the library can be logically divided into two separate physical libraries with a drive each, a seven-slot magazine each, and a pre-determined number of slots in the rear storage area of the IBM 3582. If the I/O slot is defined it can be shared.

6.10 IBM 3582 initial set-up

The following section covers some of the major items required to implement, manage, and operate the IBM 3582 tape library. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the *IBM 3582 Ultrium Tape Library Setup, Operator, and Service Guide*, GA32-0548.

6.10.1 SCSI ID

The IBM 3582 has one or two SCSI devices/addresses: the two drives. The default settings for the SCSI IDs are 0 and 1. Depending on your requirements, you may have to change the SCSI ID default settings for your installation.

The IBM 3582 uses a path through one or more of the tape devices to access the tape library robot. The tape device is LUN 0, and the library robot will be LUN 1. A SCSI ID does not have to be set for the library robot.

The IBM 3582 is a SCSI target device and it can be connected to a single-ended, Low Voltage Differential or High Voltage Differential SCSI bus. The SCSI bus must be terminated, and a terminator is shipped with each library.

6.10.2 Identifying library location element numbers

To manipulate the media within the library, the host must reference each movement with source and target designations. This is done via element addressing, which specifies precisely which slots within the library are to be used. Table 6-3 shows the element addressing scheme used for the IBM 3582 tape library.

Table 6-3 IBM 3582 element numbering

Column	Element numbers
Picker	1
I/O station	16
Drives	256 - 257
Storage	4096 - 4116

Drives are addressed from bottom to top.

The I/O station is addressed from top to bottom. Storage slots are addressed from top to bottom, column by column.

6.11 Operator displays and buttons

Normally, the host issues commands to the IBM 3582 tape library. Operator control is provided via the Operator Panel. The operator is responsible for:

- Starting the IBM 3582 tape library
- Shutting down the IBM 3582 tape library
- Handling media

ROS nº 03/2005 - CN - CPMI - CORREIOS
1496
Fls. Nº
Doc. 3690

Refer to the IBM TotalStorage Ultrium Tape Library 3582 *Setup, Operator and Service Guide*, GA32-0458, for general procedures.

6.11.1 Operator Panel

The Operator Panel provides communication between the operator and the IBM 3582 tape library. Visual indications and push buttons enable the operator to control the IBM 3582 tape library.

As shown in Figure 6-4, the IBM 3582 tape library operator panel is divided into two areas:

1. Operator Panel Keyboard:
   The Operator Panel Keyboard is a five-button keypad that lets you control the library operations interactively. Using the Operator Panel, you can set library options, check library status, and diagnose errors.
2. Operator Panel Display:
   The Operator Panel Display is an LCD on the library front panel that is used to display icons and text.

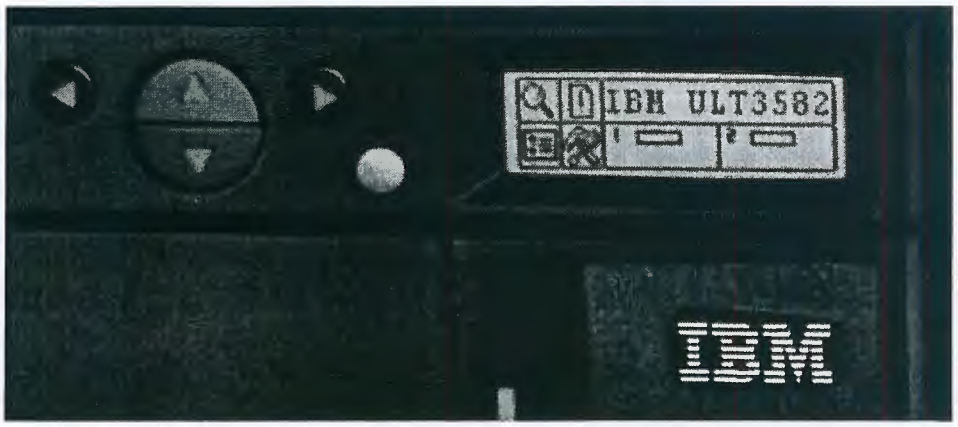


Figure 6-4 IBM 3582 operator panel

Menu options

Figure 6-5 on page 127 shows the layout of the menu options on the operator panel.

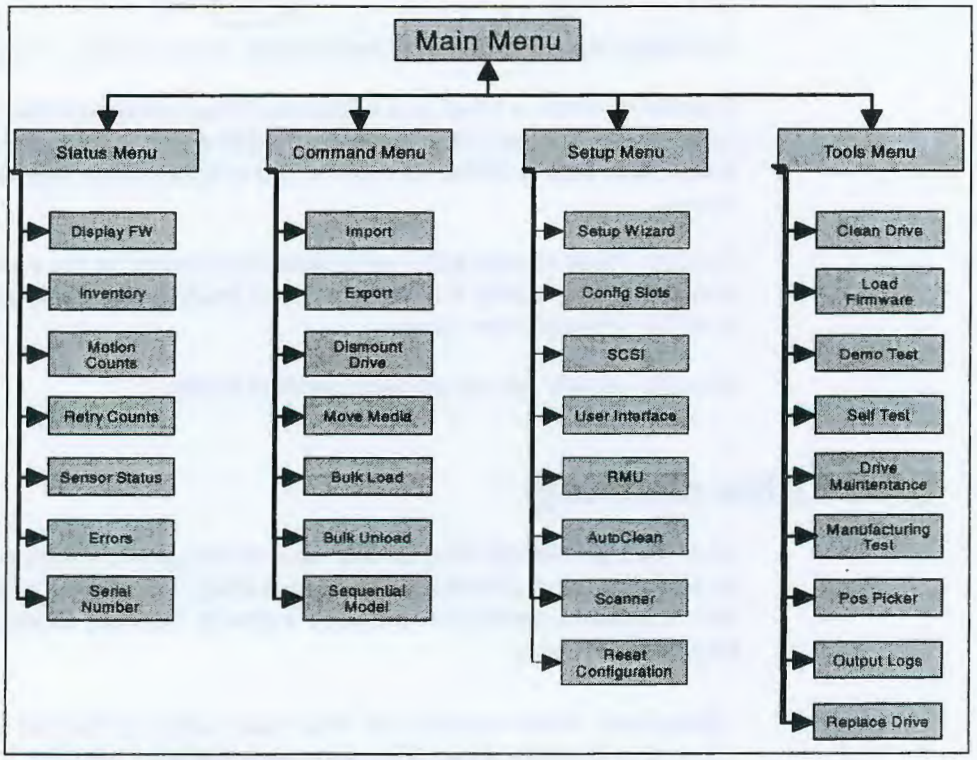


Figure 6-5 IBM 3582 top-level menu options

Each menu is accessible through the Operator Panel push buttons. Refer to the Operation chapter in the IBM TotalStorage Ultrium Tape Library 3582 *Setup, Operator and Service Guide*, GA32-0458, for all menu items.

Using commands that require an offline state

Some commands require that the library be in an offline state. If any such commands are attempted while the library is in an online state, the operator will be requested to take the library offline.

Operator intervention message

If a problem causes an operator intervention message to appear, refer to the Troubleshooting and Diagnostics section in the IBM TotalStorage Ultrium Tape Library 3582 *Setup, Operator and Service Guide*, GA32-0458.

RQS nº 03/2005 - CN - CPMI -- CORREIOS
Fls.. Nº 1497
Doc: 3690

6.12 Library mode

The library operates in one of two modes: random mode or sequential mode.

Sequential mode is used with applications that recognize the tape drives but not the medium changer. Tape cartridge locations and loading are managed by the library, and data is written to tapes in the order in which they are stored in the library.

Random mode is used with applications that recognize the medium changer and drives. The application manages the tape loading, slot positioning, and the order in which cartridges are used.

Libraries usually are set up using random mode.

6.13 Drive cleaning

All of the IBM Ultrium Tape Drives have an integrated cleaning mechanism that brushes the head at load time and again when unloading a cartridge. Drives also have a cleaning procedure that uses a special cleaning cartridge, should this become necessary.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

A specially labeled IBM LTO Ultrium Cleaning Cartridge is supplied with each IBM 3582 tape library. The drive determines when the drive head needs to be cleaned, and alerts you by displaying CT on the message display.

6.14 Firmware upgrades

Each IBM Ultrium tape drive and tape library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the current firmware is installed on your IBM LTO tape drives and library. As the IBM 3582 is designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed. Determine the latest level of firmware available from the IBM Technical Support Web site:

`http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/3582`

Follow the instructions for updating your firmware in the *IBM 3582 Ultrium Tape Library Setup, Operator, and Service Guide*, GA32-0548.

7

IBM TotalStorage Ultrium Scalable Tape Library 3583

The fourth member of the IBM Ultrium family is the IBM TotalStorage Ultrium Scalable Tape Library 3583, shown in Figure 7-1 on page 130. It is a high-performance, reliable, scalable tape subsystem. Designed for tape automation, the IBM TotalStorage Ultrium Scalable Tape Library 3583 (IBM 3583) can be attached to iSeries, pSeries, xSeries, AS/400, RS/6000, Netfinity, and non-IBM servers, workstations, and personal computers that support SCSI HVD, SCSI LVD, and Fibre Channel interfaces. It uses IBM Ultrium tape drives for fast data transfer and reliability in automated library service. Each aspect of the library subsystem has been optimized for repeated, reliable unattended tape handling.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI – CORREIOS
Fls. Nº 1498
Doc: 3690

Figure 7-1 IBM TotalStorage Ultrium Scalable Tape Library 3583

The IBM 3583 tape library houses from one to six IBM Ultrium tape drives, which can have a native data transfer rate of up to 35 MBps and a cartridge capacity of up to 200 GB, depending on whether it is an Ultrium 1 or Ultrium 2 drive. Any combination of Ultrium 1 or Ultrium 2 drives may be installed. The drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm, which provides an effective data rate of up to 70 MBps and a cartridge capacity of up to 400 GB (with 2:1 compression) on IBM Ultrium 2 200 GB media. Multiple-drive models provide additional enhanced functions such as fast transfer of data, simultaneous backup, concurrent read-write operations, Control Path Failover, and fault tolerance. The Multi-Path Architecture enables a single library to be shared by multiple homogeneous or heterogeneous applications.

The IBM 3583 models feature cartridge capacities of 18, 36, and 72 cartridges; that is, capacities of 3.2 TB, 7.2 TB, and 14.4 TB of uncompressed Ultrium 2 data. With compression (assuming 2:1), the largest model of the 3583, the Model L72, can store 28.8 TB of Ultrium 2 data.

The IBM TotalStorage Ultrium Scalable Tape Library 3583 is an excellent choice if your application is experiencing growth in online storage requirements and you are considering a tape automation solution for your data storage needs.

7.1 Model description

The IBM 3583 supports up to six IBM LTO Ultrium tape drives. It comes standard with remote library management, multi-path architecture, and the ability to partition the library into three logical libraries. The library can be configured as a stand-alone unit or can be mounted in an industry-standard 19-inch rack. Additional optional features include Control Path Failover for AIX. The Library 3583 comes in three different models. The major difference between the models is the number of storage cells shipped with the initial order:

- *IBM 3583 Model L18* is supplied with space for 18 cartridges.
- *IBM 3583 Model L36* is supplied with space for 36 cartridges.
- *IBM 3583 Model L72* is supplied with space for 72 cartridges.

The models are summarized in Table 7-1:

Table 7-1 IBM 3583 model summary

Model	Cartridge Slots	Native Data Capacity with Ultrium 1	Native Data Capacity with Ultrium 2	IBM Ultrium Tape Drives
L18	18[a]	1.8 TB	3.6 TB	1-6
L36	36[b]	3.6 TB	7.2 TB	1-6
L72	72[c]	7.2 TB	14.4 TB	1-6

a. Plus one I/O Station slot
b. Plus one I/O Station slot
c. Including twelve I/O Station slots

The model numbering is an indication of how many cartridge slots the model was originally shipped with. However, all of the IBM 3583 models are the same physical size, and the two smaller models, L18 and L36, can be field-upgraded to hold up to 72 cartridges by the addition of upgrade features. The effect of these upgrades is shown in Table 7-3 on page 142.

7.1.1 Tape drives

The IBM 3583 libraries support the IBM LTO Ultrium 2 tape drives as well as the Ultrium 1 tape drives. Both types of tape drives and cartridges can be resident in the same 3583 frame. It is mandatory to have at least one IBM Ultrium drive installed in any of the libraries. Up to five more drives may be added either on the initial order or as field upgrades.

The installed drives may be any mixture of LVD, HVD, or 2 Gbps switched fabric Fibre Channel attached up to a total of six. However, LVD, and HVD interfaces

RQS nº 03/2005 - CN - CPMI - 1499
Fls. Nº
Doc: 3690

cannot be connected on the same SCSI bus. The drives are ordered for plant or field installation using chargeable feature codes:

- Feature #8003 provides one IBM Ultrium 1 tape drive with a Low Voltage Differential (LVD) Ultra2/Wide SCSI adapter.
- Feature #8004 provides one IBM Ultrium 1 tape drive with a High Voltage Differential (HVD) Ultra/Wide SCSI adapter.
- Feature #8103 provides one IBM Ultrium 2 tape drive with a Low Voltage Differential (LVD) Ultra160 SCSI interface.
- Feature #8104 provides one IBM Ultrium 2 tape drive with a High Voltage Differential (HVD) Ultra/Wide SCSI interface.
- Feature #8105 provides one IBM Ultrium 2 tape drive with a Fibre Channel Interface.

Each IBM Ultrium tape drive contains the electronics and logic for reading and writing of data, control of the tape drive, management of the data buffer, and error recovery procedures. All tape drives are packaged as a common assembly that is a Field Replaceable Unit (FRU), designed for quick removal and replacement. The cartridge capacities are unaffected by the number of drives installed.

7.1.2 Cartridge storage

As well as the installed tape drives, the library enclosure contains cartridge storage slots that are arranged in columns (from one to three depending on the library model). Each of the three storage columns has provision for an additional fixed slot located at the top of each column. This slot is reserved for future use.

The tape cartridges are stored in removable magazines, which are installed into the columns in the library (three magazines to each column). The magazines are designed so that tape cartridges can only be inserted in the proper orientation. Once inserted, the tape cartridges will be retained in the magazine so that they remain in place even when the magazine is inverted and shaken lightly. The magazines can only be inserted one way into the mounting columns in the library.

7.1.3 Barcode reader

A barcode reader is provided as standard with all IBM 3583 models, and it does not affect the slot capacity of the libraries. The barcode reader is used during the inventory process to locate all cartridges inserted in the library. This action is repeated every time the front door is opened to ensure that the inventory is updated, should a cartridge have been manually added, moved, or removed while the door was open.

7.1.4 I/O station

This facility allows the insertion and ejection of cartridges without interrupting the normal operation of the library. There are two types of I/O station:

- The single-cartridge station, where the cartridge can be inserted or ejected by opening the I/O station door
- The 12-cartridge station, where 12 cartridges are contained in two removable magazines that can be inserted or ejected by opening the I/O station door

Models L18 and L36 have the single-cartridge I/O station for tape cartridges and can be upgraded to a 12-cartridge station by the feature #8012. The model L72 has the 12-cartridge station installed as standard equipment.

7.1.5 Robotic system

In conjunction with the library control microcode, the robotic system identifies and moves cartridges between the storage slots, tape drives, and the I/O station. It has a number of components:

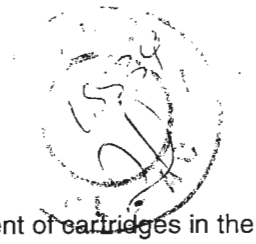
- A cartridge picker for placing cartridges in storage slots, tape drives, or the I/O station
- A barcode reader used to set up the library initially when it identifies the types of storage arrays and tape drives installed in the library, and in normal operation for reading the external labels on the cartridges, when it locates and categorizes all cartridges installed in the library
- A picker assembly for mounting the cartridge picker and the bar code scanner
- Y-axis and Z-axis drive motors for rotating the picker assembly, and moving it vertically, inside the library enclosure

7.1.6 Library control and operation

The library control unit contains the electronics and logic for autochanger operations. It controls all operations in the IBM 3583 libraries, including the interaction between the library and operators. The control unit Licensed Internal Code creates and maintains the library configuration, the physical location of the robotic system, and the inventory of cartridges. The database is kept in the flash memory of the library control hardware.

Requests issued from the server result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges to and from the tape drives and for inserting and ejecting cartridges. The host has records of the physical location of a cartridge in the library, and the physical location is also managed by the library.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1500
Doc: 3690



In addition to requesting movement of cartridges in the library, the host can obtain status, performance, configuration information, and information about the cartridges stored in the IBM 3583 tape library.

Each cartridge must have a machine- and operator-readable external barcode label to identify a media cartridge in the library during initial inventory and any time a cartridge is added to the library. The library stores the physical location of the cartridge in an inventory database based on the cartridge label. All host application requests for operations involving movement or use of a cartridge need only reference the physical location of the cartridge (using an element number as described in 7.11.3, "Element numbers" on page 150) for the library to perform the request.

7.1.7 Operator panel

An LCD operator control panel on the front of the machine provides status information and menu options. From this panel the operator can initiate actions such as moving and loading tape cartridges or invoking diagnostics.

7.1.8 Remote Management Unit

The Remote Management Unit (RMU) feature provides connectivity to Ethernet 10/100 LAN systems including Simple Network Management Protocol (SNMP). It allows library control, and configuration from authorized network attached consoles via a Web browser.

7.1.9 Library partitioning

The IBM 3583 library multi-path architecture (see 2.6, "Multi-path architecture" on page 46 for more information) allows homogeneous or heterogeneous open systems hosts to share the library's robotics without storage management middleware or a dedicated server acting as a library manager.

The library can be partitioned into as many as three logical libraries in order to share the library between different software platforms and applications (such as Windows 2000 and UNIX). Partitioning in this way means that they are able to share the library robotics independently of each other. Each logical library has its own distinct drives, cartridge storage slots, and control paths. If the application supports it, both Ultrium 1 and Ultrium 2 drives and media are allowed in the same logical library. Cartridges under library control are not shared between logical libraries, nor allowed to be moved between logical libraries. Input/output (I/O) slots are shared on a first-come-first-served basis.

For more information about the multi-path and partitioning capabilities of the IBM 3583 tape library refer to the library partitioning sections in these Redbooks:

- *Using IBM LTO Ultrium with Open Systems*, SG24-6502
- *Implementing IBM LTO in Linux and Windows*, SG24-6268

7.1.10 Multiple control paths

In addition to creating multiple logical libraries, you can also configure any logical library to have more than one control path. When you configure additional control paths, additional library sharing configurations and availability options are made possible. Access to the logical library is on a first-come, first-served basis, and each control path for a logical library can accept commands while the library is in use by another control path. By default, each logical library control path is available to servers through logical unit number 1 (LUN 1) of the first drive that is defined within that logical library.

Note: A logical unit number (LUN) is a number used by a server to identify a drive. The LUN for the Sequential Access device is always LUN 0 of the drive, and the LUN for the Medium Changer device is always LUN 1. All other LUNs are invalid addresses.

The IBM 3583 offers an optional control path failover feature that enables the host device driver to resend the command to an alternate control path; for example, to LUN 1 of the second drive in the same logical library. With control path failover installed, the alternate control path can include another HBA, SAN, or library control path drive. The device driver initiates error recovery and continues the operation on the alternate control path without interrupting the application. Only AIX hosts are currently supported for this feature.

7.1.11 SAN Data Gateway Module

The SAN Data Gateway Module (feature #8005) functions as an interface between LVD SCSI Ultrium 1 tape drives (#8003) in the library and Fibre Channel devices on the SAN. It provides attachment support for Fibre Channel interfaces using a Shortwave Gigabit Interface Convertor (GBIC) with SC connectors. The SAN Data Gateway Module is manageable over the IP network. It has an Ethernet 10/100 interface with an RJ-45 connector.

7.1.12 Maintenance

The cartridge storage slots, cartridge picker, and tape drives are accessed for maintenance purposes by opening the front door of the library. The tape drives,

RQS nº 03/2005 - CN - CPMI - CORREIOS
1501
Fls. Nº
3690
Doc:

power supplies, and host interface board are accessed from the back of the library for maintenance.

7.2 Feature codes

The IBM 3583 can be ordered and/or upgraded with the feature codes in Table 7-2. We have not included cabling options; refer to the product publications for detailed information about configuring and ordering the IBM 3583.

Table 7-2 IBM 3583 feature codes

Feature	Description	Comment
1450	Multi-Path - Field Specify	Field only
1660	RMU/StorWatch™ Specialist	Field only
1680	Control Path Failover for AIX	Automatic control path failover to a pre-configured redundant control path in the event of the loss of a host adapter or control path drive, without aborting the current job in progress
8001	IBM LTO Ultrium 100 GB Data Cartridge	Plant only, see Media section for details.
8002	IBM Ultrium Cleaning Cartridge	Plant only, see Media section for details.
8003	LTO Ultrium 1 LVD Drive Sled	
8004	LTO Ultrium 1 HVD Drive Sled	
8005	SAN Data Gateway Module	Attachment support for Fibre Channel interfaces using a Shortwave 2 GBps Gigabit Interface Convertor (GBIC) with SC connectors. LVD SCSI attachment is via a VHDCI connector.
8006	Rack mount option	
8007	18-slot Tape Storage Column	Adds 18 slots Maximum: - Model L18: two - Model L36: one
8008	Redundant power module	Redundant DC power module

Feature	Description	Comment
8010	20-pack of IBM LTO Ultrium 100 GB Data Cartridges	
8012	12-cartridge I/O station	Adds 18 slots in the door (12 of them can be used for non-disruptive exchange of cartridges) Maximum: - for L18 and L32: one - standard on L72
8013	6-cartridge magazine	Plant only
8101	IBM LTO Ultrium 200 GB Data Cartridge	Plant only, see Media section for details.
8103	LTO Ultrium 2 LVD Drive Sled	
8104	LTO Ultrium 2 HVD Drive Sled	
8105	LTO Ultrium 2 Fibre Drive Sled	
8110	20-pack of IBM LTO Ultrium 200 GB Data Cartridges	Plant only, see Media section for details.
9210	Attached to HP-UX	
9211	Attached to Sun	
9212	Attached to Windows	
9213	Attached to other non-IBM	
9215	Attached to Linux System	
9400	Attached to AS/400	
9450	Multi-Path - Plant Specify	Plant only
9600	Attached to AIX	

7.3 Physical attachments

In each of the different IBM 3583 tape library models, the interface (LVD, HVD, or Fibre Channel) on each of the drives is chosen by selecting the appropriate drive type (indicated by feature code numbers: #8003 for an LVD Ultrium 1 drive, #8004 for an HVD Ultrium 1 drive, #8103 for an LVD Ultrium 2 drive, #8104 for an HVD Ultrium 2 drive, and #8105 for a FC Ultrium 2 drive).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1502
Doc: 3690

The IBM 3583 tape library can be attached to the iSeries, pSeries, xSeries, AS/400, RS/6000, RS/6000 SP systems, Netfinity and non-IBM servers, workstations, and personal computers that support the Ultra/Wide SCSI HVD, Ultra2/Wide SCSI LVD, and Fibre Channel interface.

SCSI or FC cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code should also be specified.

The IBM 3583 may be compatible with other servers, operating systems, and adapters. Contact your local IBM representative for a current list of supported configurations. You may also refer to the Interoperability Matrix (List of Supported Servers) on this Web site:

`http://www.storage.ibm.com/tape/lto/3583/3583opn.pdf`

Another resource is the IBM SSG HBA & SAN Interoperability Matrix on:

`http://ssddom02.storage.ibm.com/hba/hba_support.pdf`

7.4 Cabling

Cables are required to attach tape drives in the IBM 3583 to each server connection (up to the number of tape drives installed).

An interposer also may be required for attachment to various server adapters. One or more of the following Fibre Channel or SCSI cables should be specified on the IBM 3583.

7.4.1 Fibre Channel cables

A Fibre Channel cable is required to attach an IBM 3583 with the San Data Gateway Module feature (#8005) or the Fibre Drive feature (#8105) to host Fibre Channel adapters, switches, or other Fibre Channel components. The short-wave, multimode GBICs that are installed in the San Data Gateway Module are SC Duplex connectors.

Note: When feature #8005 is ordered as a plant feature, one of the no-charge features #9706 (5 m SC-SC Fibre Channel cable) or #9707 (7 m LC-SC Fibre Channel cable) can be selected to provide the fiber optic cable needed to connect to the host Fibre Channel adapter. When feature #8005 is ordered as an MES feature, one of the cables listed below should be ordered if needed.

The IBM LTO Ultrium 2 Fibre Tape Drive (#8105) comes with an LC Duplex connector. One 2 m LC-LC Fibre Channel drive-to-patch panel cable is included with each Fibre Drive feature (#8105).

Additional FC cables are available as optional features on the IBM 3583 for Fibre Channel attachment to host Fibre Channel adapters, Fibre Channel switches, or other Fibre Channel components:

- Feature #5907 - 7 m SC-LC Fibre Channel Cable
- Feature #5913 - 13 m SC-LC Fibre Channel Cable
- Feature #5922 - 22 m SC-LC Fibre Channel Cable
- Feature #5961 - 61 m SC-LC Fibre Channel Cable
- Feature #6005 - 5 m LC-LC Fibre Channel Cable
- Feature #6013 - 13 m LC-LC Fibre Channel Cable
- Feature #6025 - 25 m LC-LC Fibre Channel Cable
- Feature #6061 - 61 m LC-LC Fibre Channel Cable

7.4.2 SCSI cables

A host-to-library SCSI cable is available as no-charge feature #9704 or #9705 only with the initial IBM 3583 order. One of these cables is supplied with each library ordered. Features #9704 and #9705 cannot be ordered later as an MES; however, the same cables can be ordered after installation as chargeable MES upgrades by using feature codes #5305 and #5604. Feature #9704 supplies a 4.5 m SCSI cable with an HD68 connector at one end and a VHDCI connector at the other end; feature #9705 supplies a 5 m SCSI cable with HD68 connectors at each end.

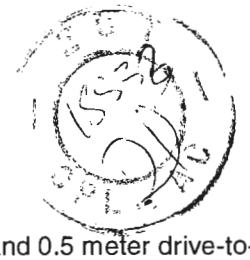
Additional SCSI cables are available as optional features for LVD and HVD attachment to host adapters. These cables have HD68 connectors on both ends:

- Feature #5302, 2.5 m (8.2 feet) SCSI cable
- Feature #5303, 0.7 m (2.3 feet) SCSI cable
- Feature #5305, 5 m (16.5 feet) SCSI cable
- Feature #5310, 10 m (33 feet) SCSI cable
- Feature #5318, 18 m (60 feet) SCSI cable
- Feature #5325, 25 m (82 feet) SCSI cable

The following cables differ in that they have a VHDCI connector at one end:

- Feature #5602, 2.5 m (8.2 feet) SCSI cable
- Feature #5604, 4.5 m (14.5 feet) SCSI cable
- Feature #5610, 10 m (33 feet) SCSI cable
- Feature #5620, 20 m (66 feet) SCSI cable
- Feature #5625, 25 m (82 feet) SCSI cable

RQS nº 05/2005 - CN - CPMI - CORREIOS
Fls.: Nº 1503
Doc: 3690



One SCSI differential terminator and 0.5 meter drive-to-drive cable is included with each SCSI drive feature (#8003, #8004, #8103 and #8104).

7.4.3 Interposers

An interposer is required to connect host adapters that do not have HD68 connectors to the SCSI cables. The following chargeable interposers are available:

- Feature #2895 interposer to connect iSeries and AS/400 to adapter #6501.
- Feature #5099 interposer to connect a mini-68-pin VHDCI connector to the 68-pin HD68 connector on the SCSI cable. This interposer (a 0.3 m cable) has a male mini-68-pin VHDCI connector on one end and a female 68-pin HD68 connector on the other.

7.4.4 Terminator

An inline terminator is required when attaching the 3583 library to Hewlett-Packard V-Class systems with adapter A4800A.

The following inline terminator is available:

- Feature #5098, Inline HVD SCSI Terminator

7.4.5 Cable length limitations

The native Fibre Channel drive and the San Data Gateway Module are capable of 2 Gbps speed. They automatically switch to a 1 Gbps speed if they are attached to a 1 Gbps host Fibre Channel adapter, switch, or other Fibre Channel components. With 1 Gbps speed the maximum cable length is limited to 300 m (984 feet), and with 1 Gbps speed to 500 m (1640 feet).

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection (for example, one host connected to only one tape drive). If using multi-drop interconnection (such as one host connected to more than one tape drive on the same SCSI bus), then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

The overall HVD SCSI cable lengths are limited to 25 m (81 feet) using point-to-point or multi-drop interconnection. The stub length at each device must not exceed 0.2 m (0.66 feet).

15532

7.5 Upgrades and optional features

You can add MES features to each model type in the IBM 3583 family in order to add capacity in terms of drives and cartridge cells, and to add the 12-cartridge I/O station. This effectively takes the place of model upgrades as there are no upgrades available for the IBM 3583 series.

In other words, you cannot upgrade an IBM 3583-L18 to an IBM 3583-L36 or L72. Similarly, an IBM 3583-L36 cannot be upgraded to an IBM 3583-L72.

7.5.1 Upgrade features

You can expand any IBM 3583 model to the maximum capacity of the largest model (L72) with the addition of MES features.

Adding drives:
You can add IBM LTO Ultrium drives to any library model to a maximum of six drives in total. The drives may be LVD, HVD, or Fibre in any combination. To install an LVD drive, add feature #8003 (Ultrium 1) or #8103 (Ultrium 2), to add an HVD drive, add #8004 (Ultrium 1) or #8104 (Ultrium 2), and to add a Fibre drive, add #8105 (Ultrium 2).

Adding cartridge capacity:
You can add an additional 18 tape cartridge slots to either of the smaller IBM 3583 models using feature #8007. You can add one or two of these features to model L18 (for a total of 36 or 54 cartridge slots), and you can add one feature to model L36 (for a total of 54 cartridge slots).

You can install a 12-cartridge I/O station to models L18 and L36 by adding feature #8012. This feature accommodates the 12 cartridges in two six-slot cartridge magazines that are accessed by opening the I/O station door. In addition to the two magazines, this feature supplies six additional fixed slots in the library door for a total of 18 additional slots. This feature in combination with feature #8007 provides the maximum slot capacity and function for the two smaller IBM 3583 models.

Table 7-3 on page 142 shows how to upgrade the capacity of 3583-L18 and 3583-L36 libraries by adding extra 18-slot tape storage columns (feature #8007) and by adding the 12-cartridge I/O station (feature #8012). You may choose to set up the12-cartridge I/O station as storage slots or I/O slots.

CPMI - CORREIOS
Fls. Nº 1504
Doc: 3690

Table 7-3 IBM 3583 capacity upgrades

3583 model	Extra tape storage columns	Single cartridge I/O station	12 cartridge I/O station defined as storage	12 cartridge I/O station defined as I/O
L18	0	18 storage 1 I/O	36 storage 0 I/O	24 storage 12 I/O
L18	1	36 storage 1 I/O	54 storage 0 I/O	42 storage 12 I/O
L18	2	54 storage 1 I/O	72 storage 0 I/O	60 storage 12 I/O
L36	0	36 storage 1 I/O	54 storage 0 I/O	42 storage 12 I/O
L36	1	54 storage 1 I/O	72 storage 0 I/O	60 storage 12 I/O
L72	Not available	not available	72 storage 0 I/O	60 storage 12 I/O

7.5.2 Optional features

Two optional features are available:

- Feature #8006, rack mount option
  The IBM 3583 libraries can be installed either stand-alone or in a standard EIA 19-inch rack. They occupy the full width of the rack and require 14 units of rack space (24.5 in or 62.2 cm). This is the chargeable feature that provides the necessary hardware to mount the library in the rack.
- Feature #8008, redundant power module
  This chargeable feature supplies a redundant DC power module for customers requiring an extra level of back-up protection. You can order one of these features per library.

7.6 Environmental specifications

The IBM 3583 Scalable is a stand-alone, medium-sized library unit that can be placed on a desk or the floor.

IBM 3583 models have from one to six drives and up to 72 cartridge slots. The physical dimensions are:

- Width: 48.1 cm (18.9 in)
- Depth: 73.5 cm (28.9 in)

- Height: 68.5 cm (27.0 in) for a stand-alone library on casters
- Maximum weight: 116.6 kg (257 lb) with six drives and 72 cartridges

7.7 Host platforms and device drivers

The following no-charge specify codes indicate the server platform to which the IBM 3583 is attached:

- Feature #9210, attached to HP-UX
- Feature #9211, attached to Sun system
- Feature #9212, attached to Windows NT system
- Feature #9213, attached to other non-IBM system
- Feature #9215, attached to Linux system (Model L23 and H23)
- Feature #9400, attached to iSeries system
- Feature #9600, attached to RS/6000 system

A device driver is additional code on the host server platform that enables it to recognize and talk to a peripheral device (in this case, the IBM 3583). Sometimes the driver code is supplied as part of the operating system code (for example, in OS/400), sometimes a software patch is required, and sometimes the driver is installed separately from a CD or diskette (either an OS CD or provided with a vendor application).

Ultrium 1

The IBM 3583 is shipped with the device drivers to support Ultrium 1 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.2 or later
- Sun Solaris 2.6, 7, and 8
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- HP-UX 11.0
- OS/400 V4R4

Ultrium 2

The IBM 3583 is shipped with the device drivers to support Ultrium 2 drives in the following operating environments at the minimal levels shown:

- AIX Versions 4.3.3 or later
- Sun Solaris 7, 8, 9
- Windows NT 4.0 with Service Pack 6
- Windows 2000 build 2195 or greater
- Windows 2003
- HP-UX 11.0, 11.i

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1505
Doc: 3690

- OS/400 V5R1 or later
- Linux distributions: Linux Red Hat 7.2 32-bit and 64 bit Kernels, Linux Red Hat 7.3, Red Hat Advanced Server 2.1, SuSE Linux Enterprise Server Update

Tip: The device driver CD or diskette that is shipped with the IBM 3583 may not contain the device drivers with the most recent level or the device drivers for all supported systems. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

7.7.1 Device driver installation

Install the IBM device drivers for the IBM 3583 as follows:

- If you intend to use the IBM 3583 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3583.
- If you do not intend to use the IBM 3583 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide*, GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3583 with a commercial software application, IBM recommends that you install any IBM-supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples of using the Ultrium drives are given in the redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

7.8 Storage applications

The software to manage the IBM 3583 is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software vendors. A list of compatible software is available at:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1 and Ultrium 2 support, and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more detailed information of specific versions and platforms supported.

7.9 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each library order[1]. With the initial order, additional data and cleaning cartridges may be ordered as chargeable features for the IBM 3583:

- Feature #8001 provides a single 100 GB Ultrium data cartridge. It is a chargeable feature, and a maximum of 19 can be ordered.
- Feature #8002 provides a single Ultrium cleaning cartridge. It is a chargeable feature and a maximum of three can be ordered.
- Feature #8010 provides a pack of twenty 100 GB Ultrium data cartridges. It is a chargeable feature, and the maximum of one can be ordered.
- Feature #8101 provides a single 200 GB Ultrium 2 Data Cartridge. Up to 19 can be ordered. The cartridges come with a barcode label but it is not affixed.
- Feature #8110 provides a pack of twenty 200 GB Ultrium Data Cartridges with unattached barcodes labels. It is a chargeable feature, and a maximum of four can be ordered.

Note: All of the media features are available only with the initial order. They cannot be ordered as an MES feature. After the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor. Refer to Appendix A, "LTO Ultrium tape media" on page 223 for details about ordering supplies and cartridges, with or without labels.

7.10 Installation and performance considerations

iSeries configurators allow only one drive per input/output port for maximum performance. Installing more than one Ultrium tape library on an input/output port may affect drive performance.

Installing more than one Ultrium drive on a SCSI bus may affect tape drive performance. For optimal performance, it is recommended that no more than one IBM Ultrium drive be attached to an individual SCSI bus.

[1] All media and cleaning cartridges are warranted separately from the IBM TotalStorage Ultrium Scalable Tape Library 3583.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1506
Fls. Nº
Doc: 3690

Intermixing of other SCSI devices on the same SCSI bus as the IBM 3583 may affect performance of those devices.

While the IBM Ultrium tape drives provide the capability for high tape performance, other components of the system may limit the actual performance achieved. The compression technology used in the tape drive can typically double the amount of data that can be stored on the media; however, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

The weight of the IBM 3583, depending on the number of drives and cartridges, may be up to 257 lbs (116.6 kg). If more than one library is mounted in a rack, a tipping hazard could be created. Customers are advised to take necessary safety precautions when mounting the libraries in the racks.

7.11 IBM 3583 initial set-up

The following section covers some of the major items required to implement, manage, and operate the IBM 3583. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

7.11.1 SCSI ID and LUN assignment

The SCSI ID and LUN assignment in the IBM 3583 tape library depends on whether the multi-path feature is installed.

If the multi-path feature is installed, the Logical Unit Number (LUN) for the tape drive is always LUN 0, and the LUN for the Medium Changer device is always LUN 1. All other LUNs are invalid addresses.

Note: The Medium Changer SCSI ID is the same as the SCSI ID for the first drive. You can enable additional drives to optionally provide Medium Changer (LUN 1) addressing by configuring more than one logical library or by enabling additional control paths.

If the multi-path feature is not installed, the IBM 3583 tape library uses a separate SCSI device address for the robot so you will have to define a SCSI ID for the tape library unit. In this case the LUNs for both the library and the tapes are always LUN 0.

Note: Do not use SCSI ID *F* as it is reserved for internal use by the SCSI library. SCSI ID 7 is also often used by the host SCSI adapter.

The IBM 3583 consists of up to seven SCSI devices: the library and up to six drives. The default settings for the SCSI IDs are 6 for the library and 0 through 5 for the drives. Depending on your requirements, you may need to change the SCSI ID default settings for your installation.

The IBM 3583 is a SCSI target device and can be connected to a single-ended LVD or HVD SCSI bus. Both ends of the bus must be terminated and a terminator is shipped with each library. The design of an IBM 3583 enables the SCSI type (single-ended, LVD, or HVD) to be configured at the customer site via a switch located on the SCSI Interface PCBA. Although the IBM 3583 can be attached to a wide SCSI bus, it is not a wide SCSI device and its SCSI ID must be in the range of 0 to 7.

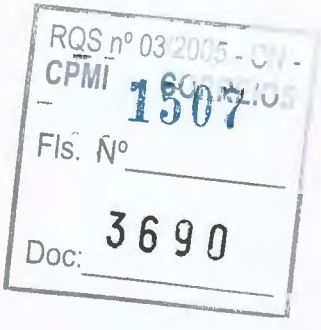
7.11.2 Identifying library locations

The convention shown in Table 7-4 is used to identify the coordinates of each library element (storage, slots, or drives).

Table 7-4 IBM 3583 storage slot coordinates

First digit	Second digit	Third digit
Column	Magazine	Row

The columns are numbered from 1 to 5 starting from the I/O station column and continuing clockwise (see Figure 7-2 on page 148).



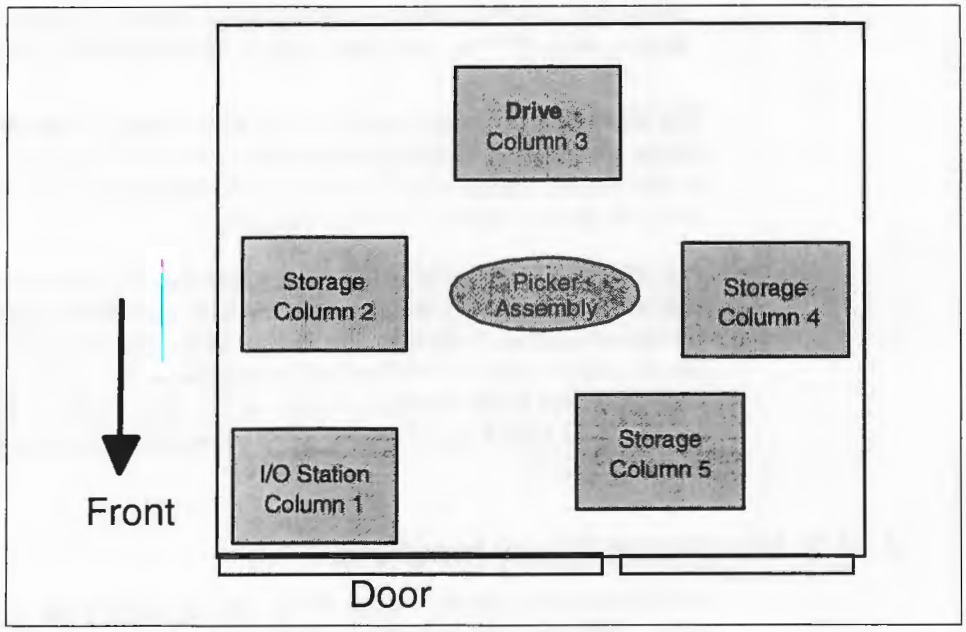


Figure 7-2 IBM 3583 storage columns: top view

The magazines within each column are designated A to C from top to bottom (label 1 in Figure 7-3 on page 149).

The rows within each magazine are numbered from 1 to 6 from top to bottom (label 2 in Figure 7-3 on page 149).

The drives within the drive column are designated from A to F from bottom to top (label 3 in Figure 7-3 on page 149).

The fixed slots in the storage columns (label 4 in Figure 7-3 on page 149) are reserved for future functions.

So, to illustrate this convention, consider the coordinates:

```
1-A-6
```

These coordinates would refer to the slot found in column 1, the top-most of the three magazines, and the bottom slot within that magazine.

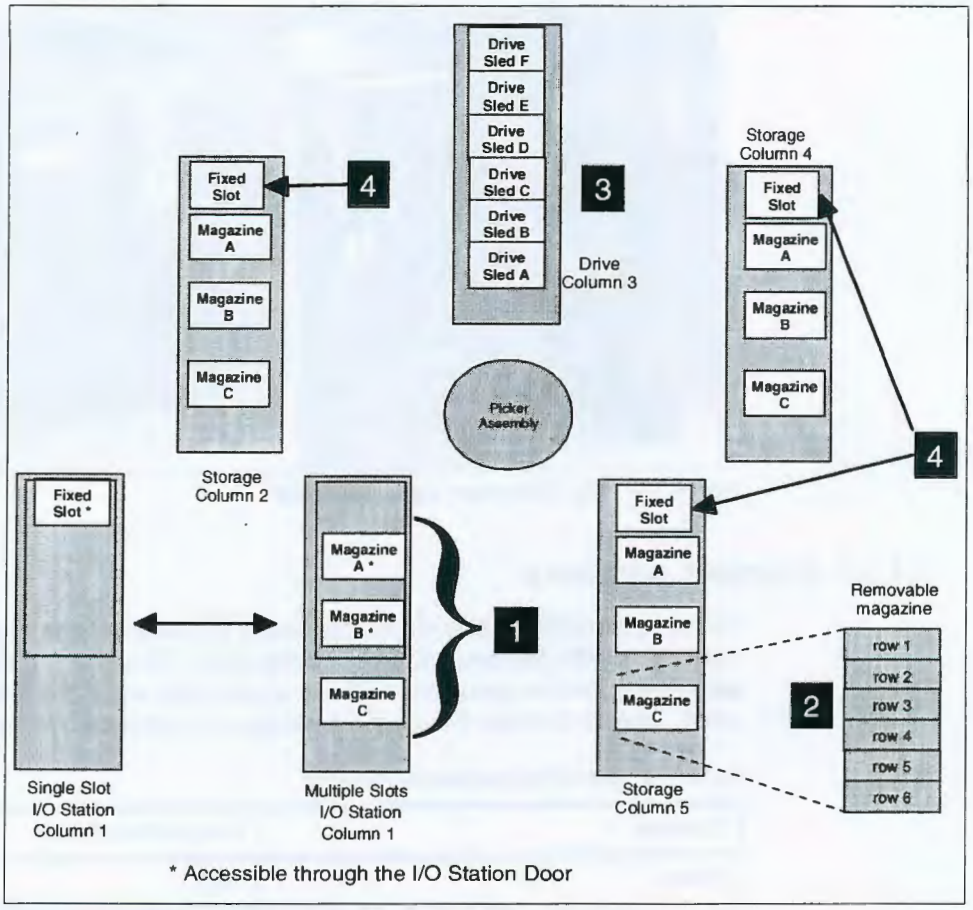


Figure 7-3 IBM 3583-L72 location logical view

Figure 7-4 on page 150 shows the actual picture of an IBM 3583 with a view of the front door opened showing I/O station column 1. This diagram also shows a good view of the 12-slot I/O station option.

Note: The only components accessible in a non-disruptive mode are the magazines located in the I/O station door (label 1 in Figure 7-4 on page 150).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1508
Doc: 3690

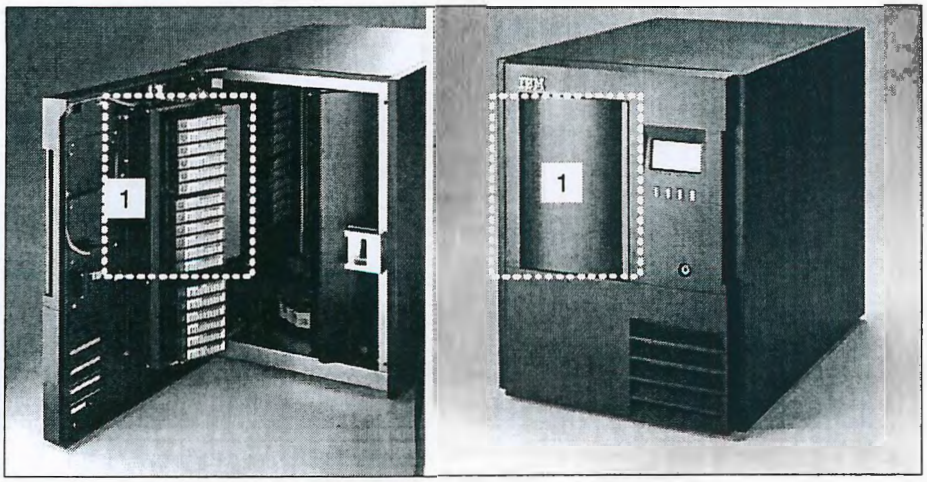


Figure 7-4 IBM 3583 front view, open door

7.11.3 Element numbers

To manipulate the media within the library, the host must reference each movement with source and target designations. This is done via element addressing, which specifies precisely which slots within the library are to be used. Table 7-5 shows the element addressing scheme used for the IBM 3583.

Table 7-5 IBM 3583 element numbering

Column	Element numbers
Picker	1h (1)
Single-Slot I/O Station	10h (16)
Multi-Slot I/O Station	10h - 1Bh (16 - 27)
Drives	100h - 105h (256 - 261)
Storage	1000h - 1047h (4096 - 4167)

Drives are addressed from bottom to top.

The I/O station is addressed from top to bottom. Storage slots are addressed from top to bottom, column by column.

7.12 Operator panel and RMU

Normally, the host issues commands to the IBM 3583 tape library. Operator control is provided via the Operator Panel or via the TotalStorage Specialist Web interface on the Remote Management Unit (RMU). The operator is responsible for:

- Starting the IBM 3583
- Shutting down the IBM 3583
- Handling media
- Updating firmware
- Cleaning drives

For detailed information about operator tasks refer to the *Operating Procedures* chapter in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

7.12.1 Operator panel

The operator panel provides communication between the operator and the IBM 3583. Visual indications and push buttons enable the operator to control the IBM 3583.

As shown in Figure 7-5 on page 152, the IBM 3583 operator panel is divided into six discrete areas:

- I/O Station status:
  The I/O Station status area provides constant information about the I/O Station (label 1 in Figure 7-5 on page 152). The information provided will state whether the I/O station is locked. The status of the I/O door and a physical representation of an occupied I/O station slot is indicated by a blacked-out area.
- Library status:
  The library status area displays informational status such as the library's online or offline status and the library reports status or messages to solicit operator intervention (label 2 in Figure 7-5 on page 152).
- Messages:
  The message area displays six lines of text, graphic representations, or a combination of both (label 3 in Figure 7-5 on page 152). Each text line can be up to 20 characters long. The display communicates interactive dialogs, special messages, alerts, and library configurations. More details are covered in Using the Operator Panel Menu in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

RQS nº 03 2005 - CN - CPMI - CORREIOS
Fls. Nº 1509
Doc: 3690

- Drive status:
  The drive status area (label 4 in Figure 7-5) provides constant information about the drives, such as:
  - Presence of tape drive (illustrated by a black outlined box for each drive)
  - Power to the tape drive
  - Cleaning requirements
  - Compression
  - Write protection
  - Tape activity
- Soft keys:
  The soft keys reference the push buttons located beneath which are used to perform commands displayed in the soft keys area and to move through the various displays of the operator panel (label 5 in Figure 7-5).
- Push buttons:
  The actual physical buttons that perform the commands referred to by the soft keys located above each one of them (label 6 in Figure 7-5).

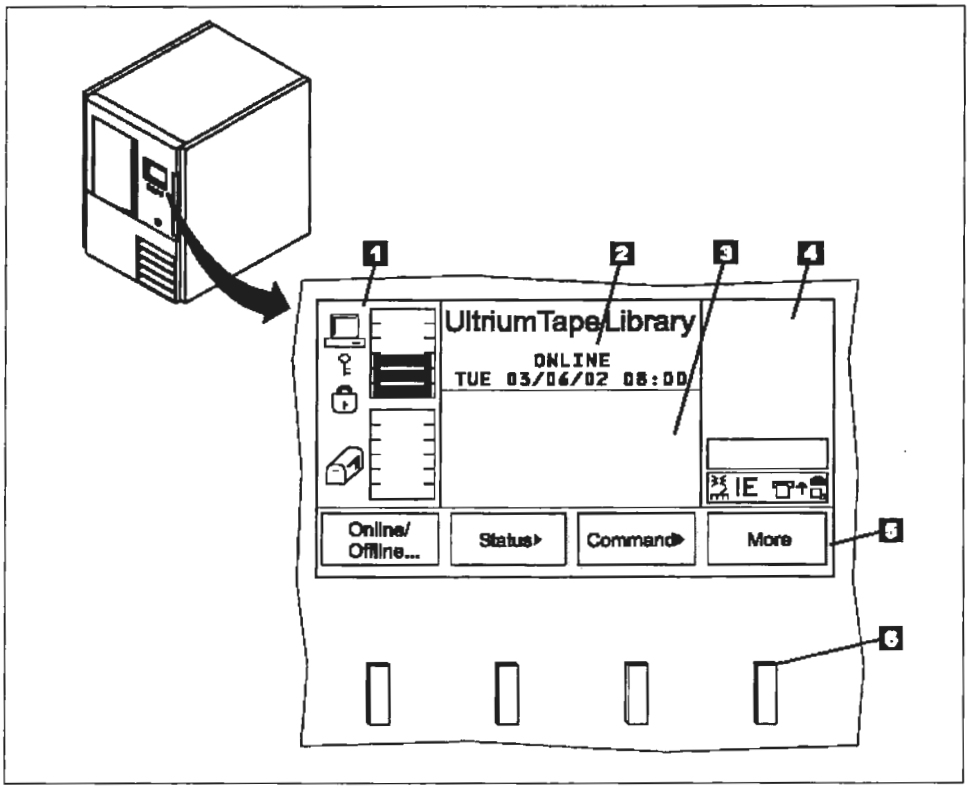


Figure 7-5 IBM 3583 tape library operator panel

Menu options

Each menu is accessible through the Operator Panel push buttons. Figure 7-6 shows the flowchart of the IBM 3583 library menu options. For more information about these functions refer to the Operating Procedures chapter in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

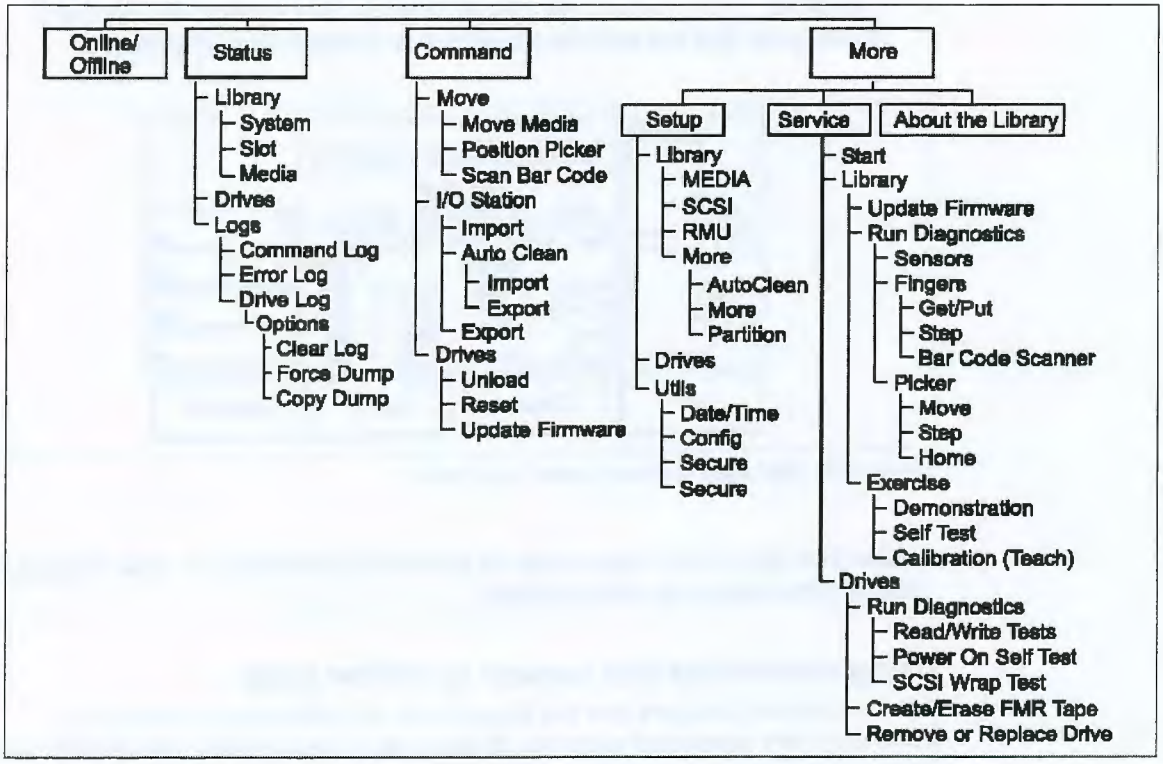


Figure 7-6 IBM 3583 flowchart of library functions

Menu guidelines

All of the the menus and their options are grouped according to function. As shown in Figure 7-7 on page 154, some options are followed by special characters, based on the following system:

- A keyword leading to another menu is suffixed by a small black arrow.
- A keyword leading to a dialog box is suffixed with three closely spaced dots.
- A keyword leading to an immediate action has no suffix.

RQS nº 03/2005 - C
CPMI - CORREIOS
1510
Fls: Nº
Doc: 3690

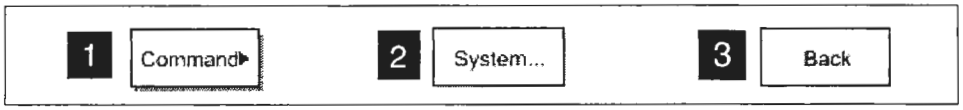


Figure 7-7 IBM 3583 soft key symbols

- Most fields on the menus, submenus, dialogs, and screens are read-only. Those fields that are writable are shown in reverse video (Figure 7-8).

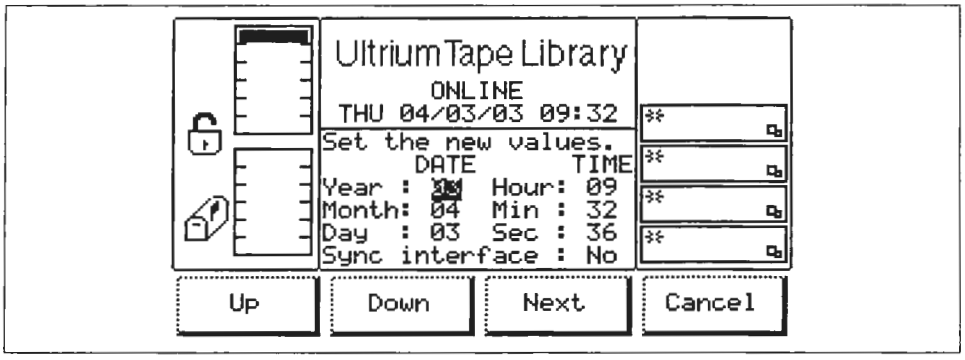


Figure 7-8 IBM 3583 operator panel: input field

Note: The information menus are not updated dynamically. To view changes, reselect the menu that was changed.

Using commands that require an offline state

Some commands require that the library be in an offline state. If any such commands are attempted while the library is in an online state, the operator will be requested to take the library offline.

Operator intervention message

If a problem causes an operator-intervention message to appear, refer to Operator Intervention Messages in the Error Messages appendix of the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

7.12.2 RMU with TotalStorage Specialist

The Remote Management Unit (RMU) provides remote access to the Ultrium Scalable Tape Library over a network. You can attach the library to the network through a 10/100 Ethernet port on the RMU. All available functions are accessible without the need of a dedicated server or separate software. You can access the library through any server on the network by entering the IP address

or IP name in a Web browser. The operator panel page of the TotalStorage Specialist Web interface is protected by a password and is a direct interface to the operator panel of the attached library.

As shown in Figure 7-9 on page 156, the IBM 3583 TotalStorage Specialist Web interface has three discrete frames:

- Left navigation:
  The left navigation frame (label 1 in Figure 7-9 on page 156) contains hyperlinks where you can log out the current user, display a brief description of the tabs from the center navigation frame, open the library's online documentation, download the SNMP MIB file, display contact information for technical support, and display the current version of the RMU firmware.
- Center navigation:
  The center navigation frame (label 2 in Figure 7-9 on page 156) has tab-style hyperlinks for Status information, Configuration, Firmware, Diagnostics file, Operator panel, and Logs. If you select a tab other than the Status tab, then you have to enter a logon name and password.
- Top information:
  The top information frame (label 3 in Figure 7-9 on page 156) contains information for you to identify the tape library that you are remotely managing. The frame shows the URL identifier and library type. The URL identifier is the hostname given to the library during initial configuration. The library type is the ID string of the library and is taken from standard inquiry data.

More details are covered in Operator Panel and RMU section in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1511
Fls. Nº
Doc: 3690

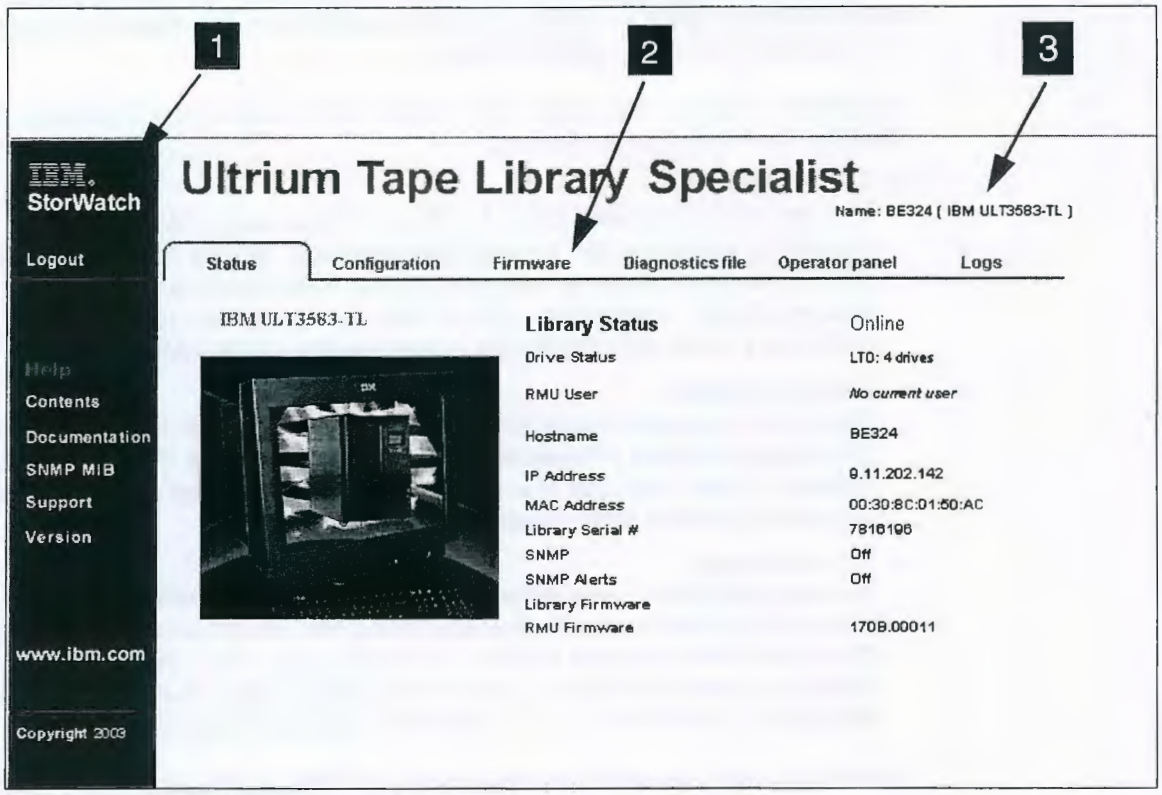


Figure 7-9 IBM 3583 TotalStorage Specialist Web interface

7.13 Random access

The library operates in random access mode, which means that you can access any cartridge in any sequence. This mode normally requires software that generates commands that are sent to the library. The server's application software manages the cartridges (and thus the data).

7.14 Drive cleaning

All of the IBM Ultrium Tape Drives have an integrated cleaning mechanism that brushes the head at load time and again when unloading a cartridge. Along with this, drives have a cleaning procedure using a special cleaning cartridge, should this become necessary.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

With each IBM 3583 tape library, a specially labeled IBM LTO Ultrium Cleaning Cartridge is supplied to clean the drive head. The drive determines when the head needs to be cleaned, and alerts you by displaying CT on the message display.

7.15 Firmware upgrades

Each IBM Ultrium tape drive and tape library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, you should make sure the current firmware is installed on your IBM LTO tape drives, library and RMU. As the IBM 3583 is designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed. Determine the latest level of firmware available from the Web site

```
http://www-1.ibm.com/support/docview.wss?rs=547&context=STCVQ6Y&q=ssg1*&uid=ssg
1S4000044&loc=en_US&cs=utf-8&lang=en+en
```

Follow the instructions for updating your firmware in the *Operating Procedures* chapter in the *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411, or from

```
http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_dri
vefw
```


CPMI - CORREIOS
Fls: Nº 1512
Doc: 3690

8

IBM TotalStorage UltraScalable Tape Library 3584

Designed for automated tape handling, the IBM TotalStorage UltraScalable Tape Library 3584 (IBM 3584) shown in Figure 8-1 on page 160 is the largest member of the IBM Ultrium family of tape library storage solutions. Each aspect of the subsystem is designed to optimize data access and reliability. IBM LTO Ultrium tape drives are compact, high-performance storage devices that support the operations required by today's network and e-business servers. The IBM 3584 supports IBM LTO Ultrium 1 and IBM Ultrium 2 drives.

The IBM TotalStorage UltraScalable Tape Library 3584 provides tape storage solutions for the large, unattended storage requirements from today's mid-range up to enterprise open systems environment. Combining reliable, automated tape handling and storage with reliable, high-performance IBM LTO Ultrium tape drives, the IBM 3584 offers outstanding retrieval performance with typical cartridge move times of less than three seconds.

The IBM 3584 can be partitioned into multiple logical libraries. This makes it an excellent choice for consolidating tape workloads from multiple heterogeneous open-system servers.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1513
Doc: 3690

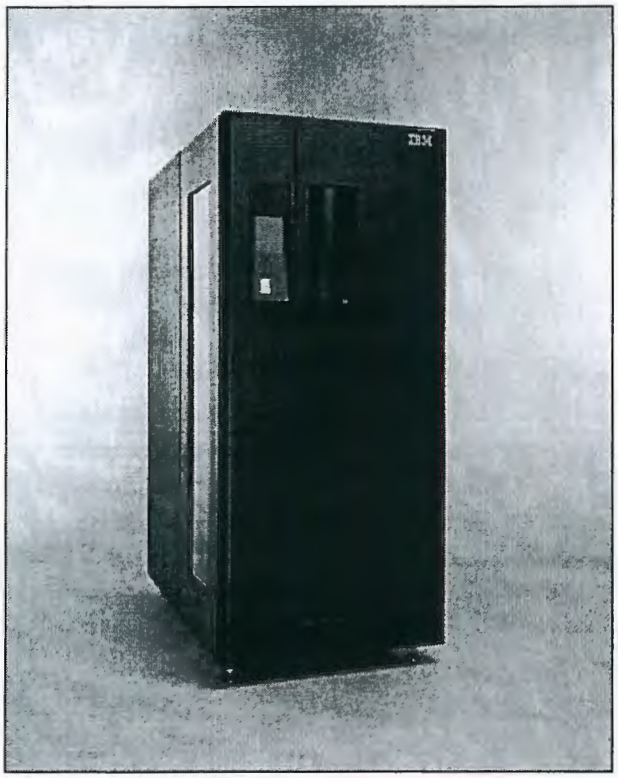


Figure 8-1 IBM 3584 UltraScalable tape library L32

The IBM 3584 is a modular tape library consisting of frames that house tape drives and cartridge storage slots. You can install a single-frame base library and add up to 15 additional frames, tailoring the library to match your system capacity and performance needs from 14 TB to 1376 TB (28 TB to 2752 TB with 2:1 compression), and using up to 192 IBM LTO Ultrium tape drives. The high granularity of the IBM 3584 library configurations, and its features and capacities are designed to match a wide variety of customer requirements.

The IBM 3584 is an excellent choice if you:

- Are experiencing rapid growth in online storage requirements
- Are considering tape autoloaders and tape libraries with software for automatic backup, archive, or fast-access tape operation to accommodate growth and reduce manual operations
- Have standardized on IBM LTO Ultrium format tape
- Are looking for an IBM LTO Ultrium tape solution requiring large cartridge capacity and fast data streaming transfer capability

8.1 Model description

Two IBM 3584 frame models can be installed together to make up the library:

- *IBM 3584 Library Unit L32*, the base frame for the IBM 3584 library, which can be installed on its own or in combination with the model D32.
- *IBM 3584 Expansion Unit D32*, up to 15 of which can be installed with the model L32 base frame. Note that the capacity expansion feature on the L32 is required (either feature #1603 or #1653) before adding D32 frames.

An IBM 3584 library can consist of a single frame (which must be the L32 model), or multiple frames, up to 16 in total. You must install a model L32 before you can add model D32s to the library, and you cannot install more than one L32 in a single library.

Note: If you are familiar with the IBM TotalStorage Enterprise Automated Tape Library 3494, then you may see that the IBM 3584 has the same form factor and looks broadly similar. However, it is *not* the same frame or internal components as the IBM 3494. You cannot mix IBM 3584 and IBM 3494 frames in the same library assembly, as the two libraries function in completely different ways.

8.1.1 IBM 3584 Library Unit L32

The IBM 3584 Library Unit L32, shown in Figure 8-2 on page 162, can be installed on its own as a complete library enclosure, or it can have up to 15 expansion frames attached to it. This frame provides the major library components for the whole library, whether it has a single or multiple frames. It also provides cartridge storage capacity and tape drives. The D32 expansion frames must be added to the right of the L32 frame.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1514
Fls. Nº
3690
Doc:

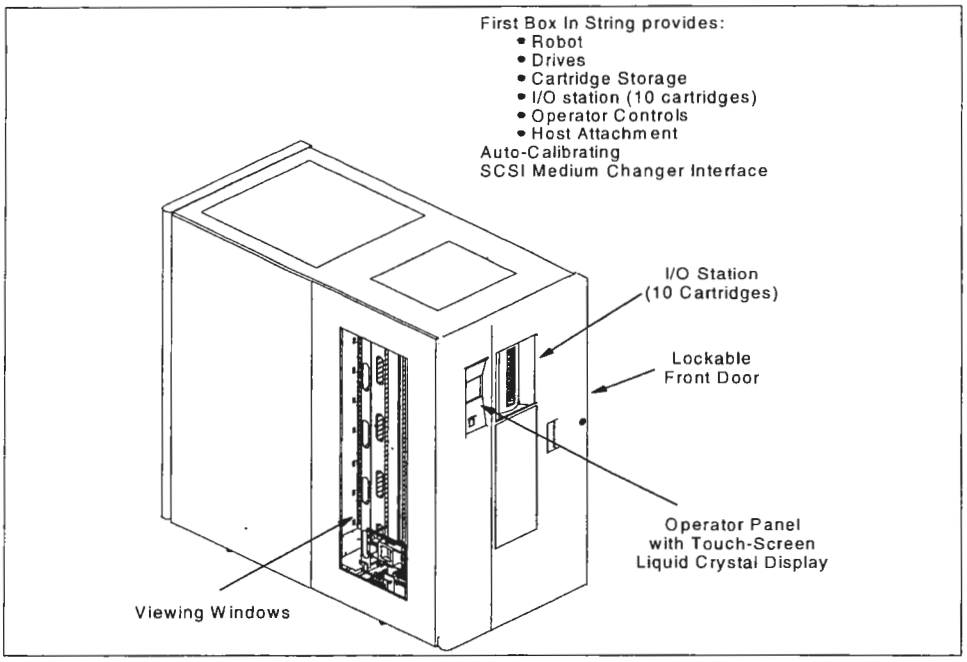


Figure 8-2 IBM 3584-L32 base frame view from front left

The number of cartridge storage slots ranges from 87 to 281, with the base frame standard of 141 slots, installed in the rear. Additional slots can be added on the door side for a maximum of 281 cartridge slots. The additional slots have to be enabled with the Capacity Expansion feature (FC #1603 or #1653), which enables use of the slots on the door. This gives a maximum data capacity for the L32 of 56 TB native (up to 112 TB with a 2:1 data compression) if you are using LTO 2 Technology. See 8.2.12, "Capacity" on page 181 for precise guidance on model L32 cartridge slot storage capacities.

At least one tape drive must be installed in the model L32 with the option to install 11 more drives for a maximum of 12 tape drives in the L32 frame. As you add drives, there is an incremental reduction in storage slots once you exceed four installed drives.

Each L32 has a standard 10-slot cartridge input/output station for importing or exporting cartridges from the library without requiring re-inventory or interruption of library operations. Optional features can provide 20 additional input/output slots. The lockable library door can be opened for bulk-loading IBM LTO Ultrium tape cartridges. Re-inventory of the cartridges is done in less than 60 seconds per frame each time the library door is closed. A barcode reader mounted on the autochanger scans the cartridge labels at less than one minute per frame. A door lock is included to restrict physical access to cartridges in the library.

8.1.2 IBM 3584 Expansion Unit D32

The IBM 3584 Expansion Unit D32, shown in Figure 8-3, cannot be installed without the L32 base frame, which must be the first frame in the library. The L32 frame also must have the capacity expansion feature (FC #1603 or #1653) installed as a prerequisite to install additional D32 frames. The D32 provides cartridge storage space and houses additional drives. Up to 15 expansion frames can be added to the L32 base frame.

When no drives are installed, the D32 has 440 installed cartridge storage slots. An L32 base frame and 15 D32 expansion frames with a minimal drive configuration provides a maximum capacity of 6881 storage slots with a total capacity of 1376 TB without compression using IBM Ultrium 2.

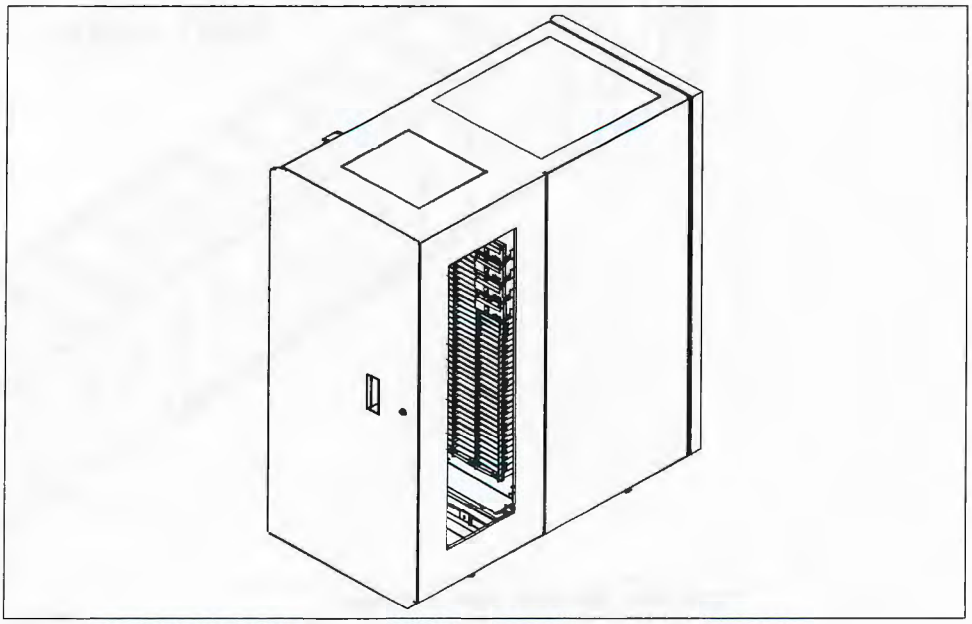


Figure 8-3 IBM 3584-D32 library expansion frame viewed from the right

Each IBM D32 houses up to 12 drives; the minimum number of installed drives is zero. In other words, you do not have to install tape drives in the model D32, but can use it solely to expand the number of storage slots in the library.

If one or more tape drives are installed in the D32 then the Frame Control Assembly Feature is also required (#1452). This feature provides the hardware and firmware required to support IBM LTO Ultrium drives within the D32, and also provides a redundant AC line feed for the L32 accessor.

ECT
CPMI 1515
Fls. Nº
3690
Doc:

The base L32 is always on the left and as many as 15 additional D32 expansion frames can be added to the right side. During the installation of additional D32 frames, the x-rail of the L32 frame where the accessor resides will be extended, so that the accessor can move through the new installed frame.

A fully configured IBM 3584 with one L32 frame and 15 D32 frames (see Figure 8-4) supports up to 192 drives. As you add drives to each D32, there is an incremental reduction of storage slots for each set of four tape drives you install.

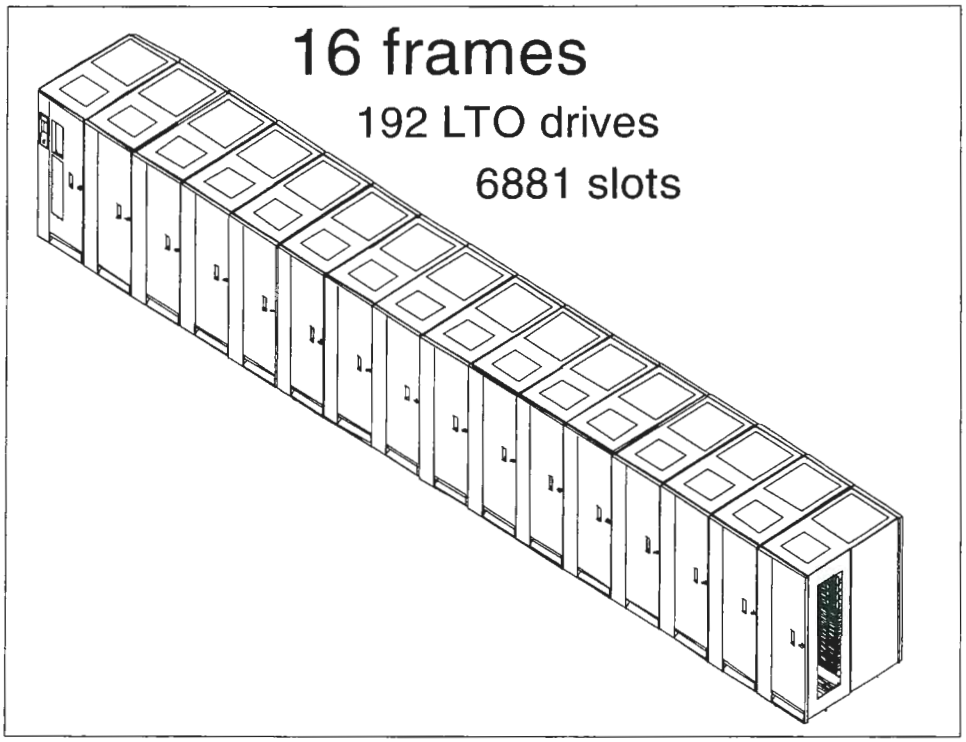


Figure 8-4 IBM 3584 with 16 frames

8.2 Library components

The major IBM 3584 library components are shown in Figure 8-5.

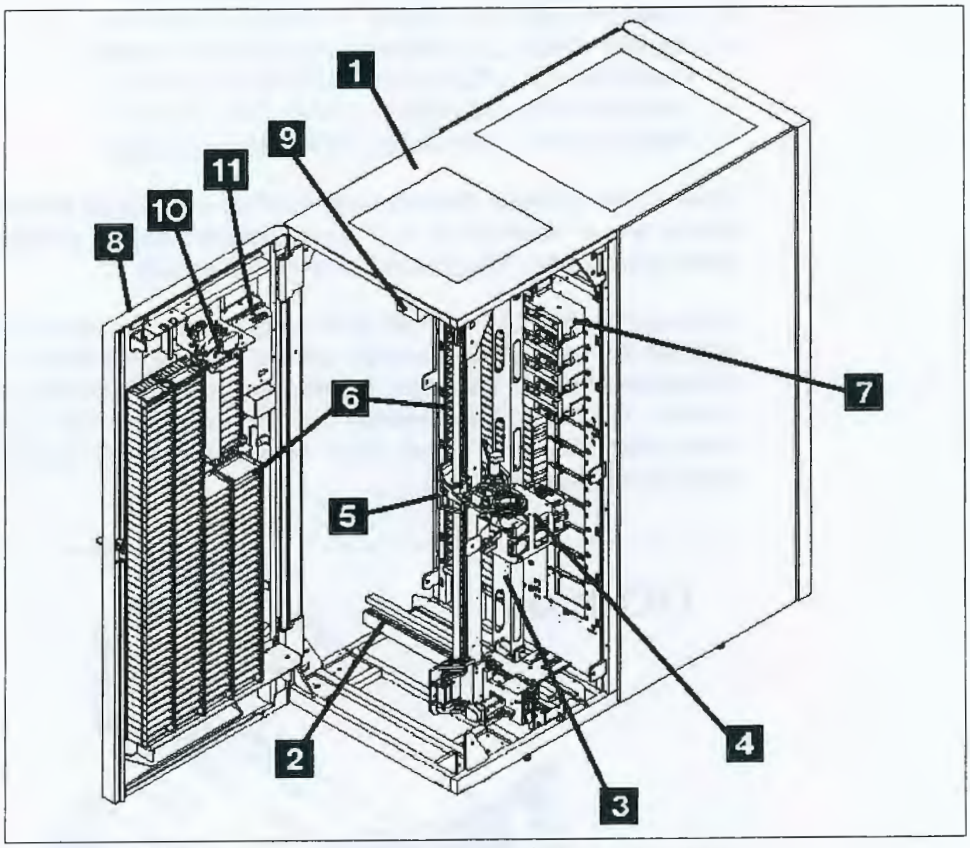


Figure 8-5 IBM 3584 library showing the major library components

1. *Library frame*
2. *x-Rail system*
3. *Cartridge accessor*
4. *Dual-gripper transport mechanism*
5. *Accessor controller*
6. *Cartridge storage slots*
7. *IBM LTO Ultrium drive*
8. *Front door*
9. *Door safety switch*
10. *I/O station*
11. *Operator panel and controller*

8.2.1 Tape drives

The IBM 3584 library houses IBM LTO Ultrium drives. Both Ultrium 1 and Ultrium 2 drives may be installed in the same frame.

CPMI - CORREIOS
Fls. 1516
Doc: 3690

IBM LTO Ultrium drives may be attached to a SCSI host system using HVD, LVD, or FC connectors. The particular drive interface is specified by the ordering feature code on the IBM 3584 model type:

- Feature #1454, LTO Ultrium 1 LVD Drive Canister
- Feature #1455, LTO Ultrium 1 HVD Drive Canister
- Feature #1456, LTO Ultrium 1 FC-AL Drive Canister
- Feature #1474, LTO Ultrium 2 LVD Drive Canister
- Feature #1475, LTO Ultrium 2 HVD Drive Canister
- Feature #1476, LTO Ultrium 2 Fibre Drive Canister

At least one of these drive features must be ordered on the initial L32 for a new library, and a maximum of 12 of these features may be added to each library frame model type. The features may be intermixed.

Although the IBM LTO Ultrium drive modules are the same for all IBM LTO libraries, the tape drive assembly used in the IBM 3584 libraries (Figure 8-6) is packaged uniquely. Therefore, the drives cannot be interchanged between library models. The tape drive assembly contains the drive power supply and the LTO drive (HVD, LVD or FC) itself. Each drive power supply is strong enough to support two tape drives.

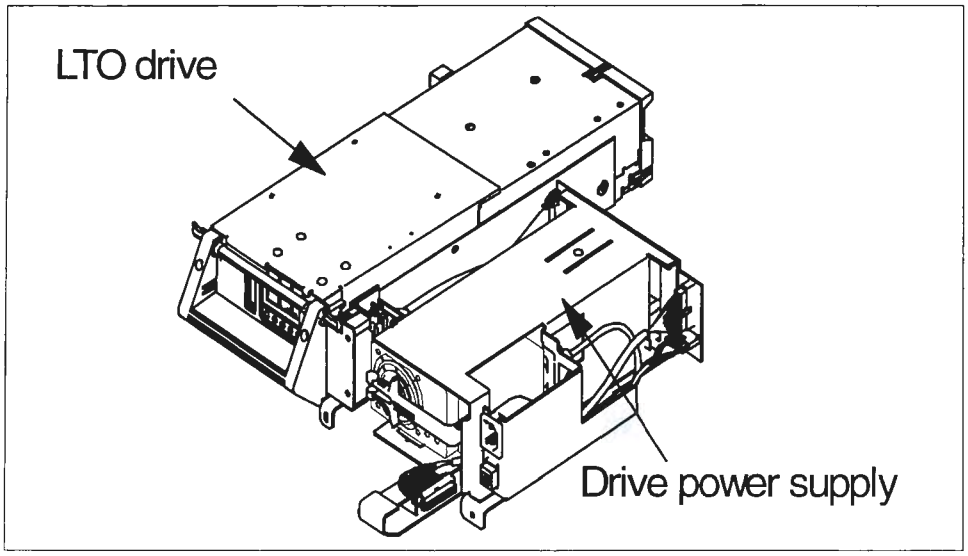


Figure 8-6 IBM 3584 LTO Ultrium tape drive assembly

For redundancy reasons, two drive power supplies deliver power for each two drives, as shown in Figure 8-7 on page 167. If one drive power supply fails, then the second power supply provides power for both drives, and both drives continue running.

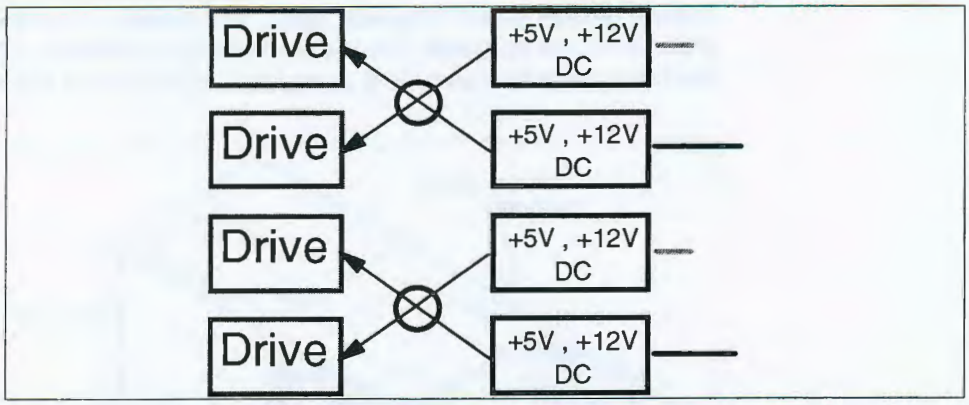


Figure 8-7 Redundant drive power supply

8.2.2 Library control systems: frame control assembly

A library control system is required for a library to operate. Conventional libraries, such as the IBM 3494, use a single library controller that handles all of the different inputs and controller output commands. The IBM 3584 uses a system of distributed embedded controllers. There are controllers, each with its own processor, for the operator panel, the accessor controller that handles the accessor and gripper, XY controller for the X and Y movements and medium changer controller for handling the commands coming from the host (Figure 8-8).

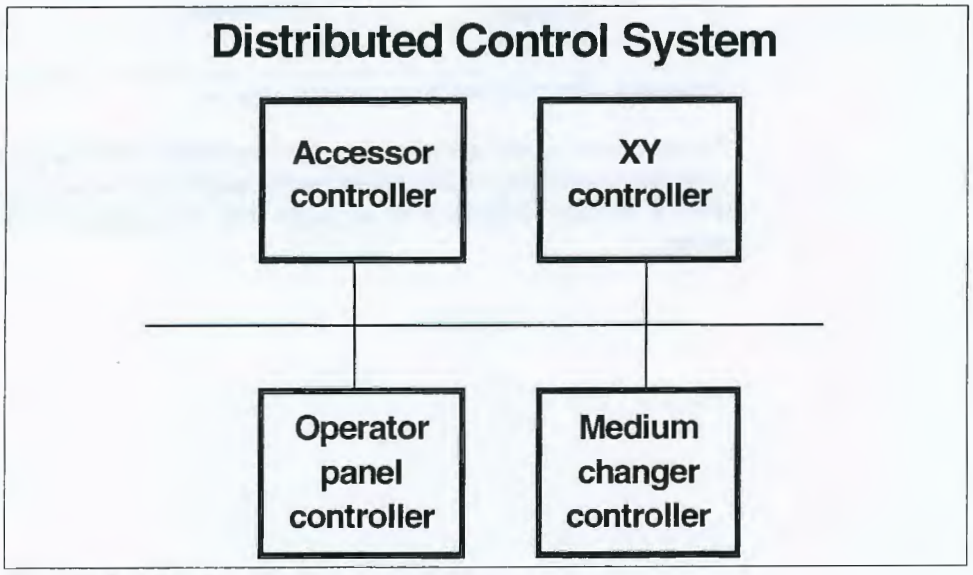


Figure 8-8 IBM 3584 distributed control system

RQS 03/2005 - CN - CPMI - CORREIOS
Fls. 1517
Doc: 3690

The four controllers are in different locations. The operator panel controller is located directly on the Operator Panel. The accessor and XY controllers are attached to the accessor. The medium changer controller, which is hosted within the frame controller assembly, is mounted in the rear of the frame (Figure 8-9).

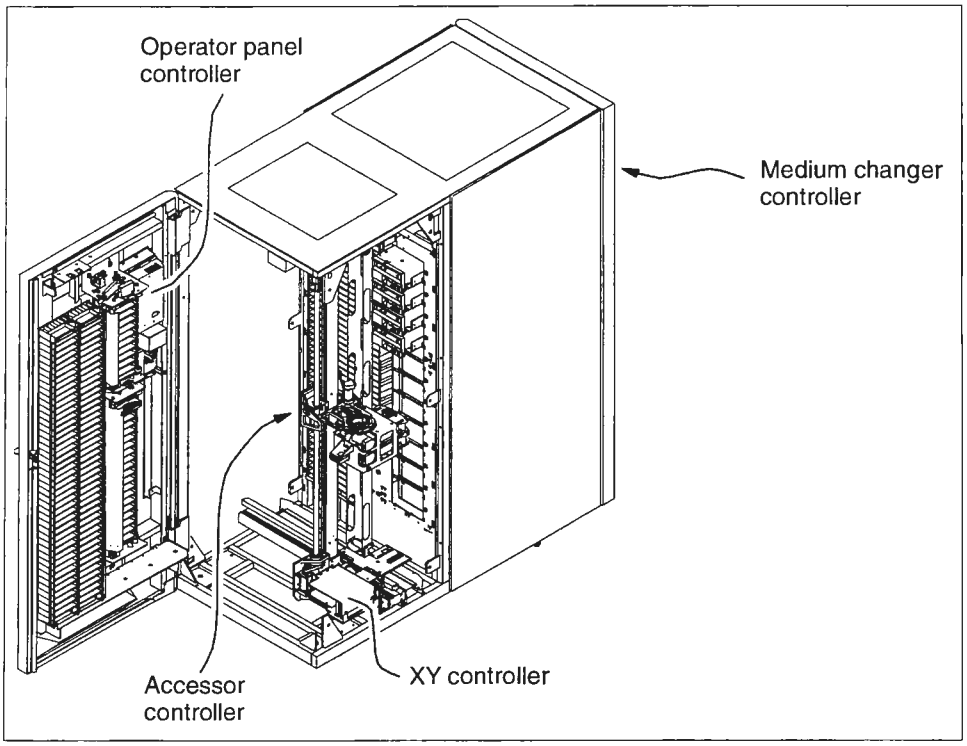


Figure 8-9 IBM 3584 distributed control system

For redundancy, the medium changer controller, which is part of the frame controller assembly (FCA), is required in each D32 frame where at least one tape drive is installed (Figure 8-10 on page 169). It is optional in a D32 with no tape drives.

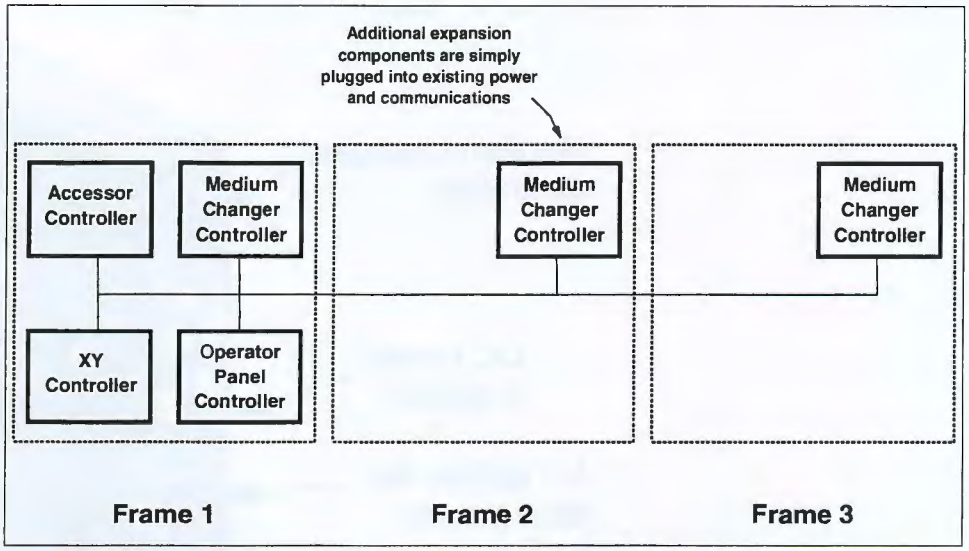


Figure 8-10 Redundant medium changer controller

The frame controller assembly (FCA) (see Figure 8-11 on page 170) is a canister containing:

- Medium changer controller
- AC outlets for tape drive power supplies
- DC power supplies for the whole library controlller
- Circuit breakers
- Incoming main AC power

The FCA for the L-Frame contains two DC power supplies; actually, only one DC power supply is needed to operate the whole IBM 3584 library. Before support was provided for 16 frames, all additional FCAs in D-Frames included one extra DC power supply for redundancy. With support for 16 frames, the additional FCAs in the D-Frames no longer have a default-installed DC power supply.

With support for 16 frames, however, you can order additional DC power supplies (FC #1902) for the D32 frames. This makes sense if not using the Dual AC power options (FC #1901); see 8.5.4, "Power and cooling specifications" on page 191. If you wish, an IBM Customer Engineer can put one of the two DC power supplies from the L-Frame into another FCA in a D-Frame to provide redundancy for both AC and DC power.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1518
Doc: 3690

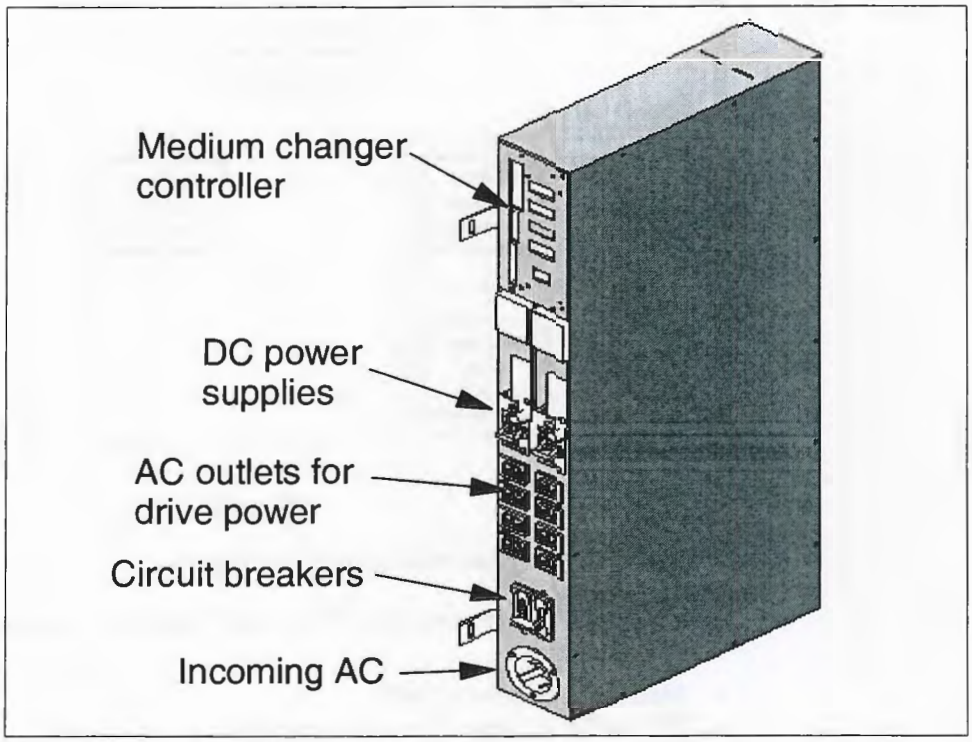


Figure 8-11 Frame controller assembly

The advantages of a distributed control system are:

- Improved reliability
  - Reduces single points of failure
  - Smaller FRU components
- Simplified library repair
  - Functionality is isolated to a single area of the library.
- Easier upgrades
  - Distributed components only require power and communication wires.
  - Modular design for "building block" approach.
- More performance than a single library controller
  - Each major library component has its own processor.

8.2.3 Operator interface

The operator interface is located on the front of the L32 frame (see Figure 8-2 on page 162) and provides a set of indicators and controls that allows an operator to perform operations and determine library status. The panel consists of the library power switch, a power-on indicator, a touch-screen LCD and controller, and the

controller for the I/O station. The operator panel controller is located inside the library behind the operator panel (number 11 in Figure 8-5 on page 165). It is a logic card that facilitates communication between the operator panel and the accessor controller. The operator panel controller posts status and information about the sensing and locking of the I/O station to the operator panel LCD.

The operator panel touch screen (Figure 8-12) consists of the touch keys area and the activity and status screen. The activity screen displays *LmultCD* on the touch screen when the library is ready (that is, when host applications may interact with the library). The first line on the screen shows the current level of library firmware and the panel screen number. The left field on the second line indicates that the library is either ready, not ready (not interacting with host applications), or initializing. The right field indicates the status of one or more I/O stations. The activity screen also shows the current activity in a large font, and provides a history of preceding operations in a smaller font. Operations are listed from top to bottom with the most recent at the top. The activity screen automatically displays an error message when an error condition is detected. See 8.9, "Operator displays and buttons" on page 196 for more information.

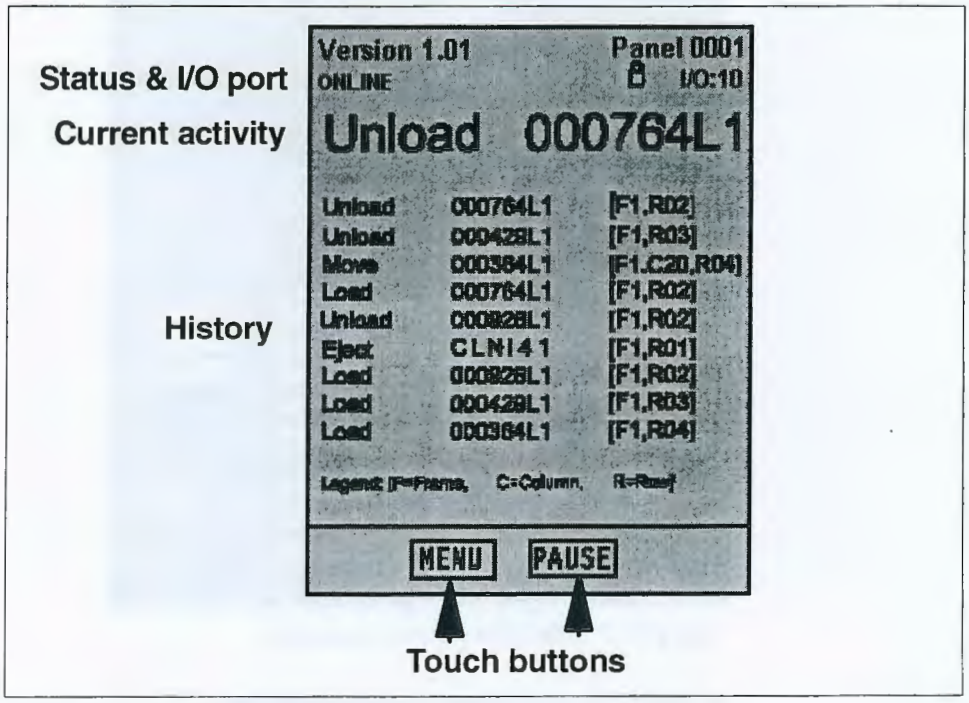


Figure 8-12 Operator panel

8.2.4 Robotic cartridge accessor

The cartridge accessor is the assembly that moves tape cartridges between storage slots, tape drives, and the I/O station (number 3 in Figure 8-5 on page 165). The accessor assembly moves horizontally through the library frames using a rail system (number 2 in Figure 8-5 on page 165); it uses both top and bottom rails.

The accessor assembly consists of a dual gripper (number 4 in Figure 8-5 on page 165 and in more detail in Figure 8-13) mounted on a vertical pole. The gripper can move up and down vertically, and also rotates to access cartridge slots on both the back walls and front doors of the library frames. A barcode reader is mounted on the accessor and can scan the cartridges in one frame in less than a minute.

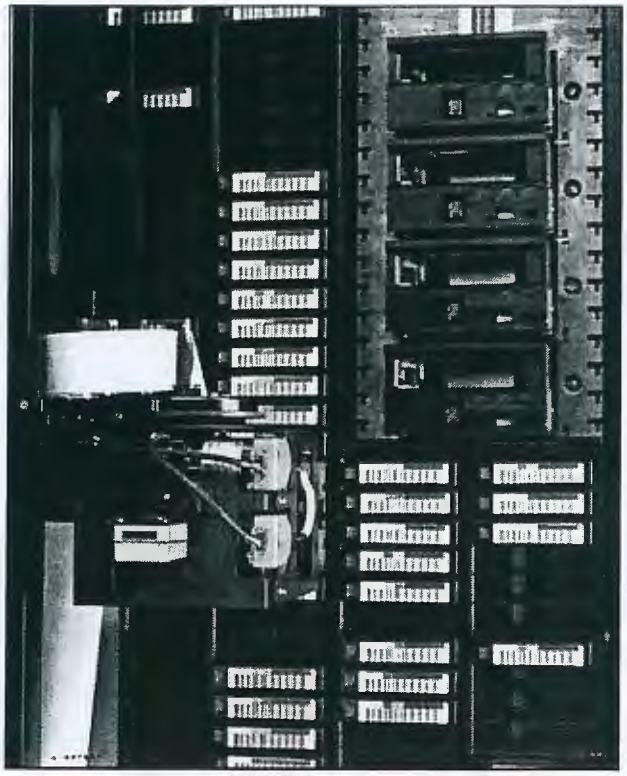


Figure 8-13 IBM 3584 accessor assembly

X- and Y-axis motion assemblies

These assemblies include a controller (circuit board) for the Controller Area Network interface, servo motor, pinion drive gear, and lead screw. These assemblies provide the motive force to move the accessor side to side (on the

X-axis) and up and down (on the Y-axis). The controller part of this assembly is referred to as the XY controller.

Pivot assembly

This group of parts provides a mounting platform for the gripper mechanism and the barcode reader. This assembly is capable of 180-degree rotation around the vertical axis.

Cartridge gripper

This electromechanical device (mounted on the pivot assembly) gets or puts cartridges from or to a storage slot, tape drive, or I/O station. The gripper is independently controlled and can grip a single cartridge. There are two grippers on the pivot assembly (Gripper 1 and Gripper 2).

Many libraries offer support for different drives and media, such as LTO, DLT, or AIT. Typically, they use a universal gripper for cartridge handling; clam shell grippers are a common design approach. The main problem with this approach is performance and reliability. A "catch-all" gripper cannot be optimized for each different media type. The LTO cartridge was designed with automation in mind, and IBM was a key player in this effort. The cartridge contains automation handling features, such as the notches seen in Figure 8-14. The IBM 3584 gripper takes advantage of the handling features and uses hooks tor handling the cartridge. This approach offers significant performance improvements as described in 8.3, "Performance" on page 186, and is more reliable than a catch-all gripper.

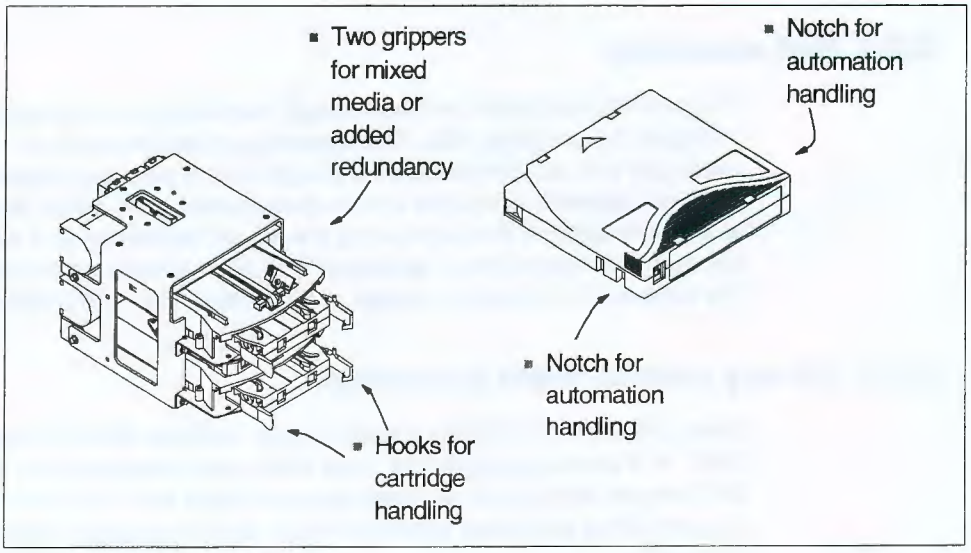


Figure 8-14 IBM 3584 Gripper

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1520
Doc: 3690

The use of a dual-gripper accessor reduces the time taken to move cartridges in the library and can improve overall performance on large libraries. It increases redundancy and reliability. Note that library functions are controlled by host application software, and to make use of the dual gripper function, the software itself must be able to use two grippers simultaneously. If it does not, then the library will function as if it had only a single gripper. If only one gripper is used at a time, the library periodically switches between both grippers to balance use.

Barcode reader

The barcode reader reads the barcode on a label that is attached to a cartridge or at the rear of every storage slot (which indicates an empty storage slot). The barcode reader is mounted on the pivot assembly, and is used during inventories, audits, insertions, and inventory updates. The inventory is updated whenever the door is opened, and determines whether cartridges have been added to, removed from, or moved within the library).

Because all storage slots have empty storage cell labels, the library can easily and quickly recognize if there is a labelled cartridge or an empty storage slot in every location. This eliminates the need to reread or manually intervene in storage cells if no label is readable. Without this approach the library cannot differentiate between a slot that is unlabeled, badly labelled, or empty.

Calibration sensor

This provides a means to locate certain positions within the library very precisely during the calibration operation. The calibration sensor is mounted on the underside of Gripper 1. All positions are calculated from these locating positions.

8.2.5 Rail assembly

The cartridge accessor moves through the library on a rail assembly (number 2 in Figure 8-5 on page 165). The system consists primarily of a main rail assembly and support rail, and a trough for the power and control cable. The main rail assembly includes a main bearing way with a rack gear. Its support rail is an L-shaped rail that runs along the top of the frames and provides smooth transport for the cartridge accessor. The power and control cable is kept clear of the accessor in a covered trough at the bottom rear of the library.

8.2.6 Library centric WWN convention

Every device in a SAN environment uses a unique WWN for identification in the SAN. In a conventional library, if the drives are swapped then the WWN will also be changed and hence you have to reconfigure both the SAN and the server. If you are using persistent binding on your server, a server reboot is also necessary.

The IBM 3584 assigns the WWNs to the drives. This technique is referred to as "library centric world wide names." Every potential drive slot is assigned with a unique WWN. If a drive is replaced, then the new drives gets the same WWN as the old one. This is controlled by the FCA. Because of this library behavior, you can easily identify the position of the drive in the library by the WWN. The last two digits represent the drive's location in the library. The last digit indicates the drive row, starting from 1, and the second last indicates the frame, counting from 0. The remaining digits are encoded with the vendor ID and the library serial number, ensuring that every drive has a unique WWN. Figure 8-15 shows the drive WWNs in an IBM 3584.

```
World Wide Node Names                    Panel 0126

Key: [F=Frame, R=Row]

[F1,R01]  5005 0763 0041 0001
[F1,R02]  5005 0763 0041 0002
[F1,R03]  5005 0763 0041 0003
[F1,R04]  5005 0763 0041 0004
[F1,R05]  5005 0763 0041 0005
[F1,R06]  5005 0763 0041 0006
[F1,R07]  5005 0763 0041 0007
[F1,R08]  5005 0763 0041 0008

[BACK]      [  UP  ]      [DOWN]
```

Figure 8-15 Drive WWNs of an IBM 3584

8.2.7 Control path failover

Alternate path support, currently available only for AIX hosts, configures multiple physical control paths to the same logical library within the device driver and provides automatic failover to an alternate control path when a permanent error occurs on one path. This is transparent to the running application.

For example, consider a simple multi-path architecture connection consisting of two HBAs in an AIX host that are connected to a library with two or more drives (Figure 8-16 on page 176). Two drives have the control ports enabled. The two HBAs are connected to the first and second control port drives, respectively. This simple configuration provides two physical control paths to the library for

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1521
Doc: 3690

redundancy if one path from an HBA to the library fails. When the AIX server is booted or **cfgmgr** is run, each HBA detects a control port to the library and two medium changer devices, smc0 and smc1, will be configured. Each logical device is a physical path to the same library; however, an application can open and use only one logical device at a time, either smc0 or smc1.

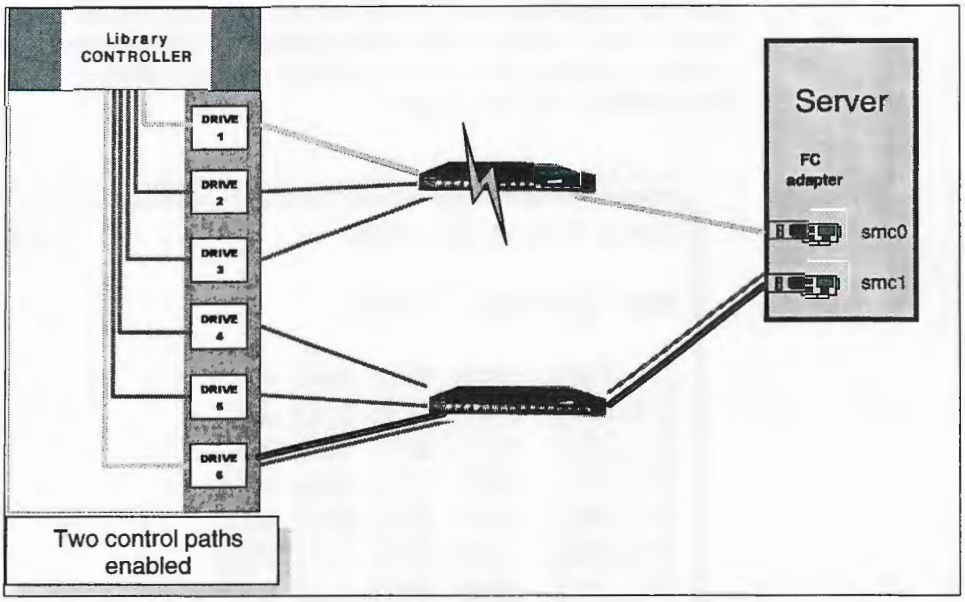


Figure 8-16 Redundant control paths to the library controller

Without the Atape (device driver) alternate pathing support, if an application opens smc0 and a permanent path error occurs (because of an HBA, cable, or drive control port failure), the current command to the library fails. It is possible to initiate manual failover by changing the device path to the alternate path (smc1), but this is a manual operation and the last failing command has to be re-sent.

When the alternate pathing support is enabled on both smc0 and smc1, the device driver configures them internally as a single device with multiple paths. The application can still open and use only one logical device at a time (either smc0 or smc1). If an application opens smc0 and a permanent path error occurs, the current operation continues on the alternate path without interrupting the application.

8.2.8 StorWatch

The library's Web interface, known as the IBM TotalStorage UltraScalable Tape Library Specialist, enables operators and administrators to manage storage devices from any location in an enterprise. The IBM 3584 StorWatch Specialist

allows direct communication with an IBM 3584 and provides a full range of end user, operator, and administrator tasks, which can be executed remotely.

The StorWatch Specialist requires a Category 5 Ethernet cable (not supplied with the tape library).

Multiple simultaneous Web clients

Each Ethernet capable medium changer controller (MCC) on the IBM 3584 allows five simultaneous StorWatch users.

Individual Web login IDs and passwords

For the IBM 3584, the Web user interface supports a list of users that can access various areas of the Web user interface. Each user has a 30-character name, a 15-character login ID, a 15-character password, and an access level. The access level defines the level of Web access that the user is allowed. The two levels of access are "user" for non-destructive Web access and "super user" for more advanced functionality such as moving cartridges and configuring the library. User and super user login IDs cannot create, modify, or change any login IDs. Any login ID can change their own password. The special login ID "admin" can create, modify, and destroy all login IDs except the admin ID.

Multiple simultaneous Web clients and individual Web ID functions can be made available to existing IBM 3584 libraries by upgrading to the latest firmware.

8.2.9 I/O station

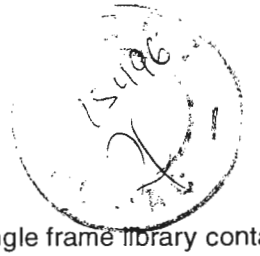
Each L32 frame has a standard 10-slot cartridge input/output station for importing or exporting cartridges from the library without requiring a re-inventory or interruption of library operations. An optional feature (FC # 1657) provides 20 additional input/output slots.

8.2.10 Reliability

The IBM 3584 is designed for high availability and reliability. Most essential components are redundant, so there is no single point of failure. Most of these components have been described previously. Here is a summary of the high-availability features and components of the IBM 3584:

- Redundant grippers
  - A failure of one gripper will cause the library to switch to a second gripper.
- Redundant library power
  - Each drive frame provides one additional power supply.

- CN - CPMI - CORREIOS Fls. Nº 1522 Doc: 3690



  - A single frame library contains one redundant power supply.
    - Optional redundant frame power available
  - The library can operate on a single power supply.
  - The library automatically monitors and controls redundant power distribution.
- Redundant drive power
  - Each drive bay power module supplies redundant power to another drive bay.
- Redundant control paths
  - Any LTO drive can be used as a library control path.
  - Automatic control path failover available for AIX.
- Redundant copies of Vital Library Data
  - Includes configuration data, calibration data, setup data, etc.
  - One processor card contains the primary copy and another processor card contains a backup copy.
  - Backup/restore process is completely automated
- Redundant copies of library firmware
  - Each processor card contains the firmware for every other processor card.
  - Component replacement is simplified.
  - Each processor card contains two copies of operational firmware.
  - Protects the library from potentially harmful firmware update disruptions.
  - Helps reduce the risk of memory failures.
- Closed loop servo systems
  - Includes horizontal motion, vertical motion, pivot motion, gripper extend, and retract motion.
  - Each servo system uses feedback.
  - Velocity and position are monitored.
  - Allows higher performance (as shown in Table 8-5 on page 187).
    - Knowing velocity and position allows greater control.
  - Closed loop is more reliable.
  - Collisions and gripper damage can be avoided by monitoring position and velocity.

15495

8.2.11 Service

This section describes support and service for the IBM 3584.

Call-home

The library calls an IBM Support Center when an error occurs. The library reports codes indicating the replacement parts that may be required and the urgency of the problem. No-charge feature #2710 (Remote Support Facility) provides a modem and cable (15.2 m or 50 feet). The customer must provide an analog phone line to use the call-home feature. This phone line should be close to the library (within 15.2 m; 50 feet).

If a second 3584 (L32) library is installed close (within 15.2 m or 50 feet) to the first one, you can order feature #2711 (Remote Support Switch) for the second library. This feature provides a modem switch in order to share the modem from the first library. The benefit is that a single phone line can service both libraries.

For the third and every subsequent 3584, installed close to the first one (within 15.2 m or 50 feet), you can order feature #2712 (Remote Support Attachment). This provides cabling for connecting to the Remote Support Switch. A maximum of 14 libraries can be connected to the switch.

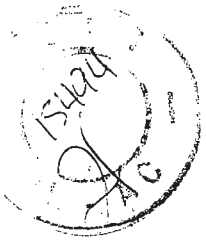
If the additional libraries are not close together, then feature #2710 and a phone line is required for each one.

Firmware

As described in 8.2.2, "Library control systems: frame control assembly" on page 167, the IBM 3584 has four control assemblies. Each of them has the complete firmware image stored on flash ROMs. The same firmware image is stored on each card, avoiding the need to keep multiple code images in sync. A node card may only use a small portion of the firmware image, but it has the whole image in its flash. The node card firmware provides the ability to communicate with other node cards. The node cards can determine the level of firmware on other node cards and can request a copy of the firmware from another node card. This ability enables the cards to operate automatically at a consistent firmware level throughout the library subsystem.

When a node card completes its Power-On Self Test (POST), it asks all of the other node cards to report their firmware levels. If it determines that another node card has a higher version of firmware, it will obtain the firmware from that node card and update its flash ROM before coming online. This ensures that when a node card FRU containing down-level firmware is installed in the library, it will be updated automatically.

RQS nº 03/2005 - CN -
CPMI - CORREIO
1523
Fls. Nº
Doc: 3690



Each node card contains two complete copies of the firmware in flash ROM for redundancy. If a problem such as a power failure interrupts a firmware update, the node card can automatically switch to the backup copy. Another attempt can then be made to update the firmware. The update process always overwrites the damaged or oldest firmware image first, so the node cards should always have a usable level of firmware.

During replacement of tape drives, the library automatically detects the firmware version of the newly installed drive and, if needed, updates the drive firmware.

This behavior of the IBM 3584 avoids any potential for replacement parts containing a wrong firmware version.

SNMP

Occasionally, the IBM 3584 may encounter a situation that should be reported, such as an open door that causes the library to stop. Because many servers can attach to the IBM 3584 by differing attachment methods, the library provides a standard TCP/IP protocol called Simple Network Management Protocol (SNMP) to send alerts about conditions (such as an opened door) over a TCP/IP LAN network to an SNMP monitoring server. These alerts are called SNMP traps. Using the information supplied in each SNMP trap, the monitoring server (together with customer-supplied software) can alert operations staff of possible problems or operator interventions that occur. Many monitoring servers (such as Tivoli NetView®) can be used to send e-mail or pager notifications when they receive an SNMP alert.

The monitoring server must be loaded with systems management software that can receive and process the trap, or the trap will be discarded. SNMP trap support does not provide a mechanism for the operator to gather more information about a problem or to query the library about its current status.

If your systems management software includes an SNMP compiler, you may not need to manually interpret SNMP traps but you will need the library's Management Information Base (MIB). The MIB contains units of information that specifically describe an aspect of a system, such as the system name, hardware number, or communications configuration. Obtain the MIB for the IBM 3584 from:

```
ftp://ftp.software.ibm.com/storage/358x/3584
```

Configuration

The IBM 3584 automatically configures and calibrates itself as initiated from the operator panel or StorWatch. New hardware is automatically discovered. This eliminates the user or IBM engineer from entering invalid data.

8.2.12 Capacity

The overall size of an IBM 3584 library frame (either L32 or D32), allows for up to 10 storage columns: five columns located on the back wall of the frame and five on the interior of the door (see Figure 8-17 on page 182 and Figure 8-18 on page 184). Each column is made up of 44 slots, so the maximum available cartridge storage capacity of the D32 frame is 440 (44 times 10).

In practice, some installed library components take up space inside the library frames, which reduces the space available for cartridge slots. Some of these library components are installed as standard (for example, in the model L32 where the maximum capacity is 281), and some are variable, for example the installation of drives in either frame model type).

This section explains the layout of the cartridge slots in the interior of each of the model types and provides tables to calculate the library capacity for various configurations.

Model L32

In the Model L32, the robotic home position utilizes the area to the left of the frame and prevents access to any cartridge slots in that area. This means that there are eight cartridge slot columns in the model L32, four on the back wall of the frame and four on the inside of the door. In addition, the I/O station takes up space on the inside of the door, and the drive positions take up space on the back wall, further reducing the cartridge slots available.

The layout of the cartridge slots and columns is shown in Figure 8-17 on page 182. The columns are numbered with those on the back wall designated as numbers 1, 3, 5, and 7, while those inside the door are numbers 2, 4, 6, and 8. Therefore column number 1 faces column number 2, 3 faces 4, and so on.

In order to provide a less expensive entry level tape solution, only columns 1, 3, 5, and 7 (those on the back wall) are accessible in the standard L32 frame. If greater capacity is needed, order a chargeable feature (the capacity expansion feature, feature codes #1603 or #1653) to make columns 2, 4, 6, and 8 available to store cartridges (noting that some of the slot positions in columns 2 and 4 are occupied by the cartridge I/O station, as shown in Figure 8-17 on page 182). The capacity expansion feature must be added before expanding the library with any D32 expansion frames.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1524
Doc:

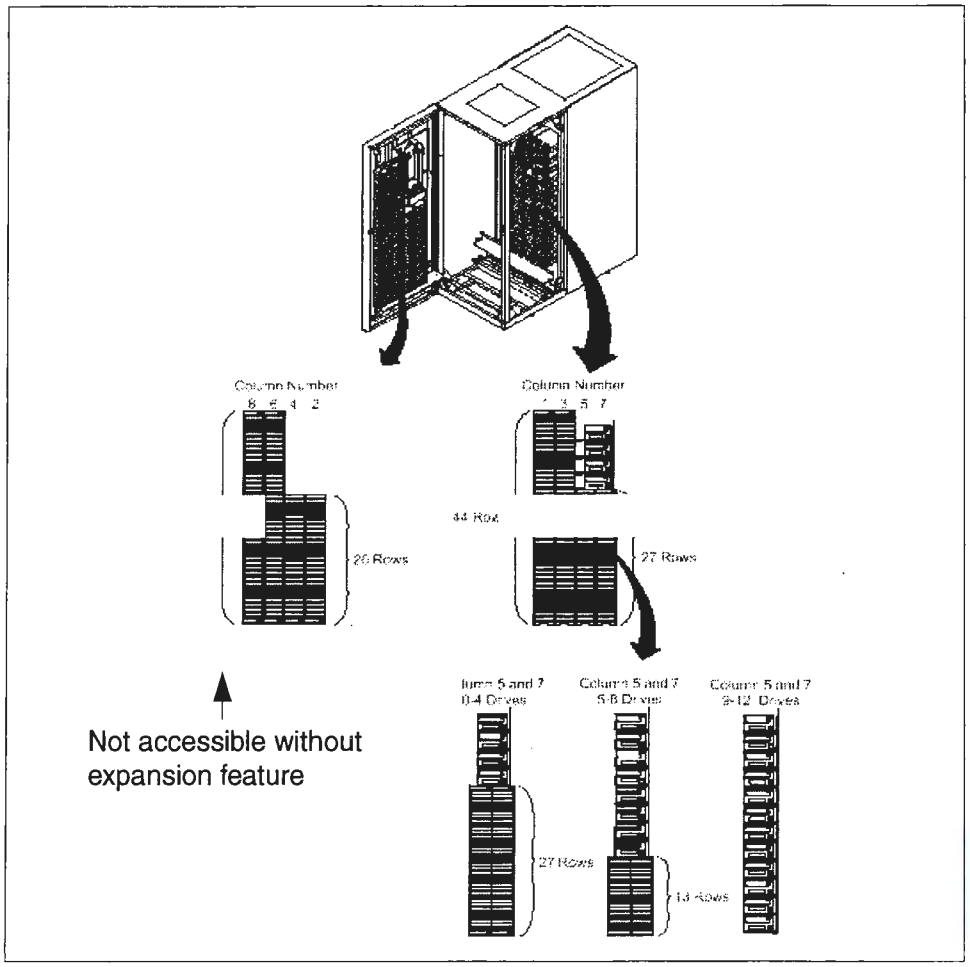


Figure 8-17 IBM 3584-L32 base frame showing cartridge slot components

The tape drives inside the L32 frame take up space in columns 5 and 7 on the right side of the back wall of the library as shown in Figure 8-17. As the drives are added, there is an incremental reduction in cartridge storage space. At least one drive must be installed in the L32 frame, and since drive positions are reserved in sets of four, this removes one-third of the cartridge slots from columns 5 and 7. When you install the fifth drive, this removes another third of the slots from columns 5 and 7, until finally, when the ninth drive is installed, the drive positions take up all of the space where columns 5 and 7 would have been located.

The very first slot in the L32 frame (column1 row 1) at the top left side of the back wall is always reserved for a diagnostic cartridge.

The next two tables summarize the available slots in the Model L32, both *without* the capacity expansion feature (Table 8-1) and *with* it (Table 8-2).

Table 8-1 IBM 3584-L32 slot capacity without capacity expansion feature

Column #	1 to 4 drives	5 to 8 drives	9 to 12 drives
1 (back wall)	43	43	43
3 (back wall)	44	44	44
5 (back wall)	27	13	0
7 (back wall)	27	13	0
2,4,6,8 (door)	Not accessible	Not accessible	Not accessible
Total	141	113	87

Table 8-2 IBM 3584-L32 slot capacity with capacity expansion feature

Column #	1 to 4 drives	5 to 8 drives	9 to 12 drives
1 (back wall)	43	43	43
3 (back wall)	44	44	44
5 (back wall)	27	13	0
7 (back wall)	27	13	0
2 (door)	26	26	26
4 (door)	26	26	26
6 (door)	44	44	44
8 (door)	44	44	44
Total	281	253	227

Model D32

In the Model D32, all 10 columns are available for use with cartridge slots. A D32 may be added to the library without any installed drives, so 10 columns of 44 slots each are available giving a total storage capability of 440 cartridges.

The columns are arranged and numbered similarly to the L32, but with two additional columns available. The layout of the cartridge slots and columns is shown in Figure 8-18 on page 184. The columns are numbered: the back wall columns are numbers 1, 3, 5, 7, and 9, while those inside the door are numbers 2, 4, 6, 8, and 10. As in the L32, column number 1 faces column number 2, 3 faces 4, and so on.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1525
3690
Doc:

All 10 columns are accessible as soon as the D32 is installed; there is no need for any capacity-expansion feature for this frame. However, note that the L32 must be fully configured for capacity before adding any model D32 frames to it. In other words, the L32 must have the capacity expansion feature installed.

The robotic home position is in the L32 and there is only one I/O station per library, which is also located in the door of the L32, so the installation of tape drives is the only factor reducing the available cartridge storage slots in the D32.

The capacity expansion feature may be ordered either for installation at the manufacturing plant as feature #1653 or as a field upgrade, feature #1603.

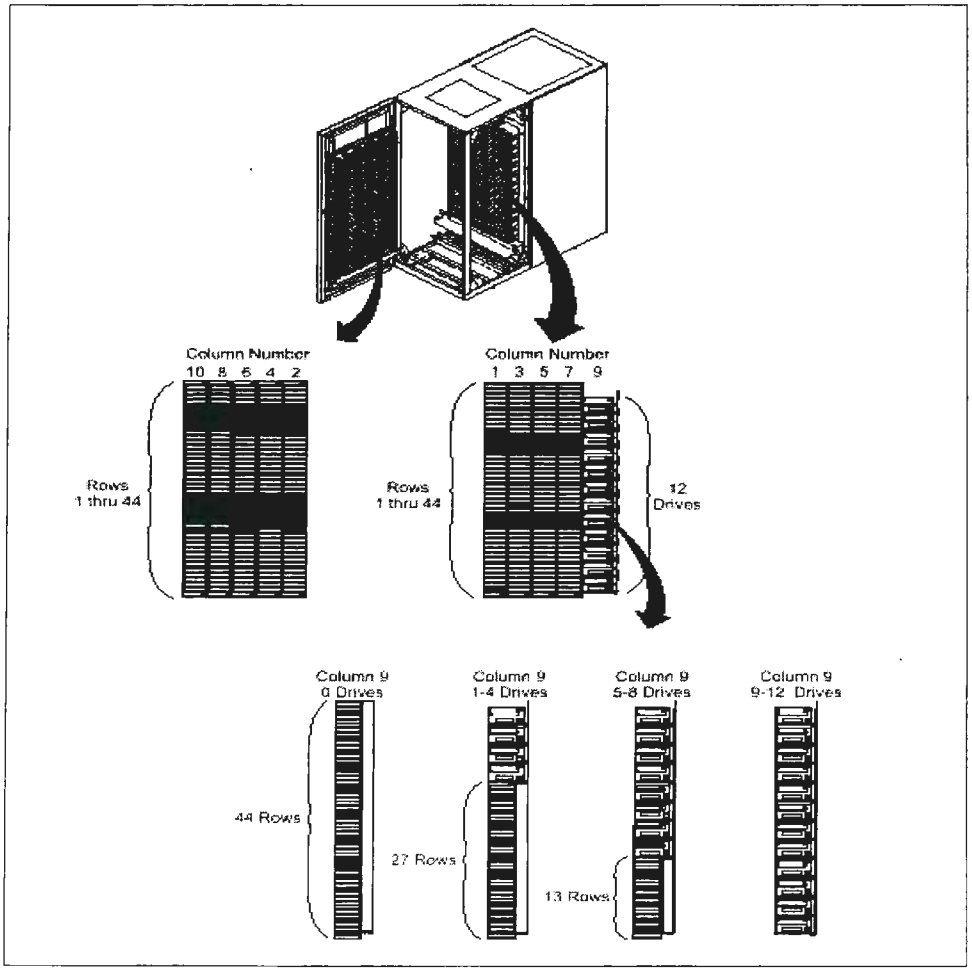


Figure 8-18 IBM 3584-D32 expansion frame showing slot components

The tape drives in the D32 are located (as in the L32) on the right side of the back wall of the library, as shown in Figure 8-18 on page 184. However, the standard layout of hardware components in the L32 differs from the D32, so space utilization is also slightly different. The tape drives in the D32 use space only in column 9 so that even with the maximum 12 drives installed, only the 44 slots in column 9 are unavailable.

As drives are installed in the D32, there is an incremental reduction in cartridge storage space in column 9. Again the drive positions are reserved in sets of four, so that installing the first drive in the frame removes one-third of the cartridge slots from columns 9. Installing the fifth drive in the frame removes another third of the slots in column 9, until finally when the ninth drive is installed, the drive positions take up all of the space where column 9 would have been located. Table 8-3 summarizes the available slots in the D32 frame.

Table 8-3 IBM 3584-D32 cartridge slot capacity

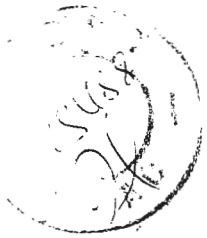
Column #	0 drives	1 to 4 drives	5 to 8 drives	9 to 12 drives
1 (back wall)	44	44	44	44
3 (back wall)	44	44	44	44
5 (back wall)	44	44	44	44
7 (back wall)	44	44	44	44
9 (back wall)	44	27	13	0
2 (door)	44	44	44	44
4 (door)	44	44	44	44
6 (door)	44	44	44	44
8 (door)	44	44	44	44
10 (door)	44	44	44	44
Total	440	423	409	396

8.2.13 Adding and removing cartridges

A 10-cartridge I/O station[1] on the front door of the IBM 3584 Model L32 enables insertion and removal of cartridges from the library enclosure without interrupting library operation. Figure 8-2 on page 162 shows the position of the I/O station from outside the library, and the internal side of the frame door is shown as number 10 of Figure 8-5 on page 165.

[1] An optional additional 20-cartridge I/O station is available.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1526
Doc: 3690



The I/O station is controlled by the host application software that uses the library or from the operator panel. Insertion of cartridges into the I/O station alerts the application software, which registers the additional cartridges and their status in its database and then instructs the accessor to move the new cartridges into library slots. The slot location of each cartridge is held in the host application software database.

For bulk-loading of cartridges (more than 10), you can open any library frame door and insert cartridges in any available slots in the frame. When the door is closed, the library will perform a cartridge inventory operation, which checks to determine whether each cartridge storage slot in the frame is empty or full and scans the cartridge barcode labels. When the library performs an automatic inventory in this way, the inventory will occur only for those frames whose doors had been opened.

A cartridge inventory operation occurs whenever you:

- Power on the library
- Issue the SCSI command Initialize Element Status with Range[2]
- Select Inventory from the Manual Operations menu
- Select the appropriate menus from the UltraScalable Specialist Web interface
- Close the front door after manually accessing the library

When the library performs an automatic inventory because the front door was closed, the inventory occurs only for those frames whose doors have been opened. A door lock is provided to restrict physical access to cartridges in the library. This can be used to secure the cartridges and prevent unauthorized library access. Although the time required for the library to inventory cartridges is less than 60 seconds per frame, the door lock reduces the possibility of frames being opened in error and causing unnecessary inventory activity.

There is also a safety switch in the frame door (number 9 in Figure 8-5 on page 165) that shuts down the power to the cartridge accessor whenever the front door is opened.

8.3 Performance

The performance capability of a tape library solution depends on both the individual bandwidth capability of the drives and data bus and the speed of the robotic handling. The degree of importance for each of these elements depends on the quantity of data transferred during one operation. For example, when reading or writing large files (larger than 800 MB) to tape, then the data rate of

[2] The 3584 library tracks the logical location of all elements in the library by performing an automatic inventory as required (thus, the SCSI Initialize Element Status command is allowed but ignored).

the tape drive will be the overriding contributor to the speed of the operation. However, for reading or writing many small files (25 MB or less) to different tapes then the cartridge move and load times become the overriding contributor.

The following elements contribute to the high-performance capabilities of IBM 3584 libraries:

- Library bandwidth
  You see the bandwidth of the IBM 3584 in Table 8-4 relating to the drive performance given in 2.4.4, "Performance" on page 35. Values in the compressed column assume a compression of 2:1.

Table 8-4 IBM 3584 bandwidth

Tape drives	LTO Ultrium 1 native	LTO Ultrium 1 compressed	LTO Ultrium 2 native	LTO Ultrium 2 compressed
72	3.8 TB/h	7.7 TB/h	9.0 TB/h	18.1 TB/h
192	10.3 TB/h	20.7 TB/h	24.1 TB/h	47.4 TB/h

- Cartridge move time
  In a single-frame IBM 3584, the typical time to move a cartridge from a cartridge storage slot to a tape drive, for example, is less than 2.5 seconds, For a six-frame configuration it only increases to 4.5 seconds, and for the maximum 16 frames, the average move time is still only 9 seconds, as shown in Table 8-5.

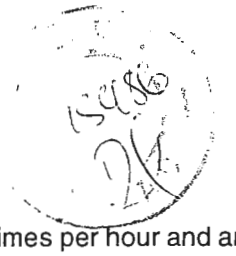
Table 8-5 Library performance

Library configuration	Average move times	Mounts per hour
1 Frame	2.4 seconds	600
2 Frames	2.5 seconds	515
4 Frames	3.0 seconds	405
6 Frames	3.8 seconds	340
8 Frames	4.9 seconds	265
12 Frames	6.5 seconds	205
16 Frames	8.0 seconds	165

Here are some thoughts about the relationship between drives per library and mounts per hour:

- If you do mainly full backups that fill entire cartridges at a time, an Ultrium 1 drive needs about 111 minutes and an Ultrium 2 about 95 minutes to fill a cartridge. This means that you have to mount an Ultrium 1

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1527
Doc: 3690



drive 0.54 times per hour and an Ultrium 2 drive 0.63 times per hour. Even in a 16-frame library with 192 drives, you should not encounter any performance problems stemming from the mount capability of the library.

- If you mount a cartridge, read or write a small piece of data, unmount the cartridge, and repeat, then a drive is busy for approximately three minutes to execute this cycle (load, search, read/write, rewind, unload). This means you might mount a cartridge not more than 20 times per hour. In this worst-case scenario, you may see mount performance affecting library performance.

Both of these theoretical cases should help you determine how many tape drives you should install in the library to avoid mount performance problems.

- Library inventory time
  During normal use of the IBM 3584, for bulk loading of cartridges the library will perform an inventory operation to check the (possibly new) content of the cartridge storage slots. During this time, the accessor is occupied scanning the bar code labels and empty slots.

  The inventory process for the IBM 3584 is performed very efficiently, usually taking less than 60 seconds per frame.

8.4 Upgrades and optional features

The IBM 3584 has a number of optional additional features. These enhance the library by providing extra functions, additional capacity, higher reliability, and greater serviceability.

8.4.1 Upgrade features

You can install an entry-level system with moderate capacity then upgrade it as capacity requirements increase by ordering extra features. A single-frame, single-drive system can be expanded over time to become a fully configured 16-frame 192-drive library.

Adding cartridge capacity

You can add capacity to an installed library in several ways:

- The #1603 capacity expansion feature can be applied to a standard model L32 (one without #1603 or #1653 already installed). This feature enables the use of 140 cartridge storage cells on the inside of the door.
- Model D32 expansion frame can be added to the base L32 frame to provide a maximum of 440 extra storage slots. To provide the full capacity you must add #9001 to indicate that the frame is to be supplied without drives[3]. Up to 15

D32 frames can be added to the base frame for up to 6,600 additional storage slots in increments of 440.

Adding drives to the library

The minimum requirement for an IBM 3584 (either single or multiple frame) is that it contain at least one tape drive in the L32 base frame.

To add a drive to the library, you can order any of these features, which can be intermixed within the library:

- Feature #1454, LTO Ultrium 1 LVD Drive Canister
- Feature #1455, LTO Ultrium 1 HVD Drive Canister
- Feature #1456, LTO Ultrium 1 FC-AL Drive Canister
- Feature #1474, LTO Ultrium 2 LVD Drive Canister
- Feature #1475, LTO Ultrium 2 HVD Drive Canister
- Feature #1476, LTO Ultrium 2 Fibre Drive Canister

The maximum number of drives per frame (L32 or D32) is 12, creating a total of 192 drives in a 16-frame library. Be aware that as you add drives to a frame, you incrementally lose cartridge storage slots (see 8.2.12, "Capacity" on page 181).

8.4.2 Optional features

For more information about available features, see the sales manual for the IBM 3584. You can access the sales manual at:

`http://www.ibmlink.ibm.com/ussman`

8.5 Environmental specifications

The IBM 3584 is designed to be a stand-alone tape subsystem consisting of one or more frames and capable of modular expansion to provide large capacities. The frames join end to end, with the base frame on the left (viewed from the front) and the expansion frames extending to the right.

8.5.1 Physical dimensions

The IBM 3584 frames have the same physical dimensions but their weights vary according to the number of installed drives, robotics, and tape cartridges:

- Width: 72.5 cm (28.5 in)
- Depth: 152 cm (59.8 in)
- Height: 180 cm (70.9 in)

[3] Adding drives to the frames incrementally reduces the capacity

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1528
Doc: 3690

Each frame has a set of casters and four leveling jackscrews. The nominal height from the bottom of the jackscrews to the top of the frame is 1840 mm (72.4 in), and can be varied by ±40 mm (±1.6 in). The shipping height of the IBM 3584 (on its casters and with jackscrews raised) is 1800 mm (70.9 in)

When planning for the installation, consider the space implications in your computer room for the possibility of adding more frames in the future.

- Weights[4]:
  - IBM 3584-L32 with 1 drive, no cartridges: 423 kg (932 lb.)
  - IBM 3584-L32 with 12 drives, 227 cartridges: 570 kg (1256 lb.)
  - IBM 3584-D32 with no drives, no cartridges: 355 kg (784 lb.)
  - IBM 3584-D32 with 12 drives, 396 cartridges: 558 kg (1229 lb.)

8.5.2 Floor requirements

Install the library on a raised or solid floor. The floor must have a smooth surface and, if raised, must not have ventilation panels beneath the leveling jackscrews. If carpeted, ensure that the carpet is approved for computer-room applications. To accommodate unevenness in the floor, you can raise or lower the leveling jackscrews to the following specifications:

- Maximum allowable variance must not exceed 7 mm (0.27 in) per 76 mm (3 in).
- Maximum out-of-level condition must not exceed 40 mm (1.6 in) over the entire length and width of the library.

The floor on which the library is installed must be able to support:

- Up to 4.8 kilograms per square cm (68.6 lb per square inch) of point loads exerted by the leveling jackscrews
- Up to 211 kilograms per square meter (43.4 lbs per square foot) of overall floor loading

The number of point loads exerted depends on the number of frames that make up the library. There are four point loads per frame (located at the corners of each frame).

[4] The weight with cartridges assumes a cartridge weight of 0.209 kg (0.460 lb) for a standard cartridge. The actual weight of the library varies, depending on the configuration and cartridge capacity.

8.5.3 Operating environment

The IBM 3584 is designed to operate in the following environment:

- Temperature: 16° to 32° C (61° to 89° F)
- Relative Humidity: 20% to 80%
- Wet Bulb: 23° C (73.4° F) maximum

8.5.4 Power and cooling specifications

Power and cooling for the IBM 3584 components are provided by the housing frame. Each base and expansion frame that contains drives has its own frame control assembly (FCA), which receives power from a customer-supplied outlet and, in turn, provides AC power to all tape drives within the frame. The FCA for the L32 contains two DC power supplies; actually, only one DC power supply is needed to operate the entire library. Before support was provided for 16-frames, all additional FCAs in D32s included one additional DC power supply for redundancy. With support for 16-frames, the additional FCAs in the D-Frames no longer have a default-installed DC power supply.

Additional DC power supplies can nevertheless be ordered or made available for extra frames, as explained in 8.2.2, "Library control systems: frame control assembly" on page 167.

The FCA is not required in expansion frames that contain no tape drives.

Each frame receives single-phase (200-240 V ac) power on its own power cord from a customer-supplied outlet. Certain countries or regions require two-phase power to achieve the 200-240 V ac required by the frame. Countries in North America have the option of operating at 100-127 V ac power (FC 9951).

A new Dual AC Power feature (FC 1901), supporting either 110 V ac or 220 V ac, is available for the IBM 3584, providing two independent line cords that may be connected to two independent customer branch circuits. A power switch connects to one of two customer power feeds and passes all AC power to the frame from that feed. The switch monitors the AC line voltage from the feed it is using and automatically switches to the alternate AC power feed if the incoming voltage drops below a preset level.

Table 8-6 on page 192 lists the power requirements for the L32 and D32 frames.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1529
Doc: 3690

Table 8-6 Power requirements for the IBM 3584

Power requirement	Model L32 or D32	
	220 V ac line cord	110 V ac line cord
AC line voltage	200 to 240 V ac (nominal)	100 to 127 V ac (nominal)
AC line frequency	50 to 60 Hz	50 to 60 Hz
Nominal power	1.4 kW	1.2 kW
Line current	8.0 A	12.0 A
kVA	1.6 kVA	1.2 kVA
Heat output	4.8 kBtu/hr	4.1 kBtu/hr
Inrush current	200 A (peak for 1/2 cycle)	100 A (peak for 1/2 cycle)

Note: Values shown for frames with 12 IBM LTO Ultrium tape drives installed.

8.6 Host platforms and device drivers

The IBM 3584 is supported on many operating systems. For a current list of host software versions and release levels that support the 3584, refer to:

`http://www.storage.ibm.com/tape/lto/3584/3584opn.pdf`

The following no-charge specify codes indicate the server platform to which the IBM 3584 is attached. These features are used by IBM for device driver distribution:

- Feature #9210, attached to HP-UX
- Feature #9211, attached to Sun System
- Feature #9212, attached to Windows System
- Feature #9213, attached to other non-IBM system
- Feature #9215, attached to Linux System
- Feature #9400, attached to iSeries System
- Feature #9600, attached to pSeries

You are not limited to one platform-attach feature as the library may be attached to more than one of these platforms. You cannot add more than one of each feature; in other words, if you have two or more Windows servers, only one feature #9212 is required. The device driver will be delivered on a CD that contains all available device drivers for each OS and the documentation.

Tip: The device driver CD or diskette that is shipped with the IBM 3584 may not contain the most recent device drivers. Always check the following FTP site for the latest device drivers:

`ftp://ftp.software.ibm.com/storage/devdrvr/`

8.6.1 Device driver installation

Install the IBM device drivers for the IBM 3584 as follows:

- If you intend to use the IBM 3584 with a commercial software application (such as IBM Tivoli Storage Manager, VERITAS Backup Exec, or Legato NetWorker), refer to that application's installation instructions to install the device driver and configure the IBM 3584.
- If you do not intend to use the IBM 3584 with a commercial software application, install the tape and medium device driver from the CD that is shipped with the drive. Refer to the installation instructions in the *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide*, GC35-0154, which is supplied on the CD with the driver code.

Note: If you use the IBM 3584 with a commercial software application, IBM recommends that you install any IBM-supplied device driver only if instructed to do so in the installation instructions supplied by the vendor of the application. Otherwise, if the application supplies its own driver code, then conflicts could occur over which driver controls the drive. Many examples are given in the Redbooks *Implementing IBM LTO in Linux and Windows*, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

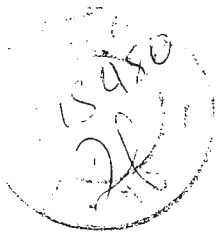
8.7 Storage applications

Software to exploit the IBM 3584 is not provided with the library. Additional software support is available through products that must be obtained separately from IBM, IBM Business Partners, or independent software vendors. A list of compatible software is available at:

`http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

You will find details for each application including Ultrium 1 and Ultrium 2 support and specific Ultrium models and attachment methods. You should also contact your storage application vendor for more information about specific versions and platforms supported. Many examples of third-party software applications with IBM LTO drives and libraries are given in the Redbooks *Implementing IBM LTO in*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls.- Nº 1530
3690
Doc:



Linux and Windows, SG24-6268, and *Using IBM LTO Ultrium with Open Systems*, SG24-6502.

8.8 IBM 3584 initial setup

The following sections cover some of the major items required to implement, manage, and operate the IBM Ultrium tapes and libraries. We do not cover all tasks, and we do not intend to cover all of the specific commands. For more details, refer to the *IBM 3584 UltraScalable Tape Library Planning and Operator Guide*, GA32-0408.

8.8.1 SCSI ID

The IBM 3584 uses multi-path architecture, so it has no direct SCSI connection to a host system. When the host communicates with the library, it must send the communication via a control path to a drive designated as LUN 1. A control path is the drive SCSI port through which a host system sends its commands to a logical library within the IBM 3584. (Refer to 2.6, "Multi-path architecture" on page 46 for an explanation of the concept of logical libraries.) When you add multiple control paths to the IBM 3584 library, any single, configured logical library can be accessed by multiple host systems.

Additional control paths also reduce the possibility that failure in one control path will cause unavailability of the entire library.

Note: The setup and SCSI configuration of the IBM 3584 are usually performed by an IBM service representative.

8.8.2 Element number

Element numbers identify the physical location within the library. This information is required mostly for storage applications, such as IBM Tivoli Storage Manager, which translate the device to a name that the robotic understands.

In the IBM 3584, each SCSI storage element is assigned a SCSI element address. A SCSI storage element is a physical location capable of holding a tape cartridge (such as an I/O slot, drive, or storage slot). The element numbering is split into three sections:

- The tape drive sequence
- The I/O station sequence
- The cartridge slot sequence

Note: The numbering is contiguous for the cartridge slot sequence. However, the addition, removal, or movement of one or more tape drives affects the element numbering of the cartridge slots.

Table 8-7 shows the element numbers for tape drives in each IBM 3584 frame up to six frames. For element numbers up to the maximum 16 frames, see the *IBM TotalStorage UltraScalable Tape Library Planning and Operator Guide*, GA32-0408.

Table 8-7 IBM 3584 tape drive element numbers

Drive number	Frame 1 (L32)	Frame 2 (D32)	Frame 3 (D32)	Frame 4 (D32)	Frame 5 (D32)	Frame 6 (D32)
1	257	269	281	293	305	317
2	258	270	282	294	306	318
3	259	271	283	295	307	319
4	260	272	284	296	308	320
5	261	273	285	297	309	321
6	262	274	286	298	310	322
7	263	275	287	299	311	323
8	264	276	288	300	312	324
9	265	277	289	301	313	325
10	266	278	290	302	314	326
11	267	279	291	303	315	327
12	268	280	292	304	316	328

Each element in the IBM 3584 (the cartridge storage slots, I/O storage slots, and tape drives) has two addresses:

- Physical address
- SCSI element address

When initiating an operation such as moving a tape cartridge or performing manual cleaning, you can use the physical or logical address to specify a location in the library.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1531
Doc: 3690

The physical address consists of frame, column, and row identifiers that define a unique physical location in the library. The address is represented as:

- Fx,Cyy,Rzz for a storage slot (where F equals the frame and x equals its number, C equals the column and yy equals its number, and R equals the row and zz equals its number).
- Fx,Rzz for a tape drive and I/O storage slot (where F equals the frame and x equals its number, and R equals the row and zz equals its number).

The SCSI element address consists of a bit and hex value that defines to the SCSI interface a logical location in the library. This logical address is represented as xxxx (X'yyy'), where xxxx is a bit value and yyy is a hex value. It is assigned and used by the host when the host processes SCSI commands. The SCSI element address is not unique to a storage slot, drive, or I/O slot; it varies, depending on the quantity of drives in the library.

For example, the storage slot address F2,C03,R22 means:

- F2: frame 2 (first expansion frame)
- C03: column 3 (second column from left on drive side)
- R22: row 22 (22nd position down from the top of the column).

Each drive has a unique address to indicate its physical location. The drive address consists of two values, a frame number and a row number:

- Frame number: Represented as Fx, where F equals the frame and x equals its number. Regardless of whether any drives are installed, the frame number for the base frame is 1 and increments by one for each adjacent expansion frame.
- Row number: Represented as Rzz, where R equals the row and zz equals its number. The row number is 1 for the top drive position in the frame, and increments by one for each row beneath the top drive. Regardless of whether drives are installed, the row numbering is the same for every frame.

A drive address of F2,R10 means frame 2 (that is, the first expansion frame), row 10 (10th drive position from the top of the column).

8.9 Operator displays and buttons

The IBM 3584-L32 operator display is a touch screen with integrated touch buttons. The display default setting will return to the basic main menu after five minutes of inactivity. The screen has three sections (Figure 8-19 on page 197):

- The menu title and panel number
- The informational section
- The selectable buttons

Navigate through the operator panels by pressing the touch screen buttons:

- BACK:
  Will take you back to the previous screen. You may need to press the BACK button several times to return to the main status screen.
- UP and DOWN:
  If you are on a menu panel, these keys will navigate up and down within the current panel, scrolling one line when pressed once. If you keep the UP or DOWN keys pressed, scrolling will speed up. The longer you hold the keys, the faster will the scrolling be.

  If you are selecting a value, the keys will increment or decrement the value.
- ENTER:
  The selected item is shown using reverse video. No action is processed until the ENTER key is pressed.

The default display is the Activity Status Display. The information in the Activity screen is replaced automatically by an error message whenever the Ultrium tape library detects that:

- A permanent error has occurred.
- A drive requires cleaning, and automatic cleaning has been enabled.
- A drive requires cleaning, and no cleaning cartridge is present in the library.

Figure 8-19 IBM 3584-L32 operator display

Other commands or options will appear on various screens. From the main activity screen, you can access the Library Main Menu by pressing the MENU key, or pause the library for maintenance operation with the PAUSE key.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1532
Doc: 3690

The PAUSE key causes the library to park the cartridge accessor in an area that gives clear access to the library's interior (if you need to open the front door). If you accidentally press the PAUSE key, wait for the 30-second time-out. The library will automatically resume operation.

Attention: If you press the PAUSE key, then open the front door, the library rejects requests for new operations.

When selecting a critical command, such as pressing the PAUSE key, a confirmation screen will be displayed. You will see a text message with two keys, CONTINUE and CANCEL. The CONTINUE key will proceed and execute your command, and the CANCEL key will return to your previous screen.

The screens on the operator panel fall into six categories:

- Library status:
  Provides information about the accessor, the cartridge locations, the drives, and the slots.
- Manual operations:
  Enables manual intervention such as cartridge movements, cleaning, and inventory.
- Settings:
  Displays and changes configuration set-up variables such as cleaning mode, date, enabling/disabling of drives, and virtual library configuration.
- Statistics:
  Reports usage information about the accessor, drives, and cleaning cartridges.
- Vital Product Data (VPD):
  Describes the library, drives, and accessor.

  This includes such information as the machine types, model numbers, serial numbers, and the level of firmware.
- Service:
  Places the library into service mode for repairs or upgrades to be carried out.

8.10 Sequential versus random access

The IBM 3584 is designed to operate only in random mode under the control of a storage application. Sequential mode is not supported.

15475
2011

9

IBM xSeries LTO tape products

The xSeries Family of servers also features IBM Ultrium Libraries. Designed for tape automation, the IBM 3607-26X Autoloader and IBM 4560SLX Tape Library can be attached to xSeries servers and other Intel/Windows servers. They use the LTO Ultrium tape drives for faster data transfer and reliability in automated library service.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03[illegible]5 - CN -
CPMI - CORREIOS
Fls. Nº 1533
Doc: 3690

9.1 IBM 3607-26X and 4560-SLX

Figure 9-1 IBM 3607-26X Autoloader

The IBM 3607-26X Autoloader houses one Ultrium 1 tape drive with a native data transfer rate of 15 MBps and a cartridge capacity of 100 GB. The drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm, which provides an effective data rate of up to 30MBps and a cartridge capacity of up to 200 GB (with 2:1 compression) on Ultrium 1 media.

The IBM 3607-26X has one I/O slot and a cartridge capacity of 16 slots, allowing a native capacity of 1.6 TB of uncompressed data. With compression (assuming 2:1), the 3607-26X can store 3.2 TB of data.

The IBM 3607-26X Autoloader is an excellent high-performance, entry-level choice for small to midrange systems.

Table 9-1 3607-26X Autoloader model summary

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	Ultrium 1 tape drives
3607-26X	16[a]	1.6 TB	3.2 TB	1

a. Plus one (1) I/O Station slot

Figure 9-2 IBM 4560-SLX Modular Tape Library

The IBM 4560-SLX Modular Tape Library houses up to two Ultrium 1 tape drives in a module.

Ultrium 1 drives have a native data transfer rate of 15 MBps and a cartridge capacity of 100 GB. The Ultrium 1 drives feature data compression hardware using an adaptation of the IBM LZ1 compression algorithm that provides an effective data rate of up to 30 MBps and a cartridge capacity of up to 200 GB (with 2:1 compression) on Ultrium 1 media.

The IBM 4560-SLX has one I/O slot and a cartridge capacity of 30 slots allowing a native capacity 3 TB of uncompressed data. With compression (assuming 2:1), the 4560-SLX can store 6 TB of data.

The IBM 4560-SLX provides excellent tape storage scalability for mid range to high-end xSeries systems. It is expanded by configuring additional modules with the Elevator Link Option and the Elevator Link Extension Option. These features allow the library to grow to eight modules in total. This provides a maximum slot capacity of up to 240 slots when all eight modular units are installed. The Elevator options allow the library to pass cartridges between the modules, increasing the number of slots.

Table 9-2 4560-SLX Modular Tape Library with Ultrium 1 drives

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	Ultrium 2 tape drives
4560-SLX	30[a]	3TB	6TB	2

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1534
Doc: 3690

Model	Cartridge slots	Data capacity (native)	Data capacity (compressed)	Ultrium 2 tape drives
4560-SLX with one expansion module	60	6TB	12TB	4
4560-SLX with seven expansion modules	240[b]	24TB	48TB	16

a. Plus one I/O Station slot
b. Plus eight I/O station slots

9.1.1 Tape drives

The 3607-26X uses one LTO Ultrium 1 tape LVD drive. The 4560-SLX can use up to two Ultrium 1 tape LVD drives per module. The drive part number is:

- Ultrium 1 Drive - P/N 59P6658

If Fibre Channel connectivity is required for the 4560-SLX, a Fibre Channel Card Adaptor (P/N 59P6657) can be installed into the library.

Each Ultrium tape drive contains the electronics and logic for reading and writing data, control of the tape drive, management of the data buffer, and error recovery procedures. All tape drives are packaged as a common assembly that is a Field Replaceable Unit (FRU), designed for quick removal and replacement.

9.1.2 Barcode reader

A barcode reader is provided as standard with the 3607-26X and 4560-SLX, and it does not affect the slot capacity of the libraries. The barcode reader is used during the inventory process to locate all cartridges inserted in the library. This action is repeated every time the front door is opened to ensure that the inventory is updated if a cartridge has been manually added, moved, or removed while the door was open.

9.1.3 I/O station

This facility allows the insertion and ejection of cartridges without interrupting the normal operation of the library. There is a single-slot I/O station where a cartridge can be inserted or ejected by opening the I/O station door.

1547

9.1.4 Robotic system

In conjunction with the library control microcode, the robotic system identifies and moves cartridges between the storage slots, tape drives, and the I/O station. It has several components:

- A cartridge picker for placing cartridges in storage slots, tape drives, or the I/O station
- A barcode reader used to set up the library initially when it identifies the types of media and tape drives installed in the library, and in normal operation for reading the external labels on the cartridges when it locates and categorizes all cartridges installed in the library
- X-axis and Z-axis drive motors for rotating the picker assembly, and moving it horizontally, inside the library enclosure

9.1.5 Library control and operation

The Library Control Unit contains the electronics and logic for autochanger and library operations. The Library Control Unit controls all operations in the library, including the interaction between the library and the operators. The control unit Licensed Internal Code creates and maintains the library configuration, the physical location of the robotic system, and the inventory of cartridges. The database is kept in the flash memory of the library control hardware.

Requests issued from the server result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges to and from the tape drives and for inserting and ejecting cartridges. The host has records of the physical location of a cartridge in the library, and the physical location is also managed by the library.

In addition to requesting movement of cartridges in the library, the host can obtain status, performance, and configuration information, as well as information about the cartridges stored in the tape library.

Each cartridge must have a machine- and operator-readable external barcode label to identify a media cartridge in the library during initial inventory and any time a cartridge is added to the library. The library stores the physical location of the cartridge in an inventory database based on the cartridge label. All host application requests for operations involving movement or use of a cartridge need only reference the physical location of the cartridge (using an element number as described in 9.9.1, "Identifying library locations element numbers" on page 207) for the library to perform the request.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1535
Doc: 3690

9.1.6 Operator panel

An LCD operator control panel on the front of the machine provides status information and menu options. From this panel the operator can initiate actions such as moving and loading tape cartridges or invoking diagnostics.

9.1.7 Maintenance

The cartridge storage slots, cartridge picker, and tape drives are accessed for maintenance purposes by opening the front door of the library. The tape drives, power supplies, and host interface board are accessed from the back of the library for maintenance.

9.2 Library options

The following part numbers can be used to order features for the libraries (Table 9-3). We have not included the various cabling options. Refer to the product publications for detailed information about configuring and ordering the IBM Libraries, or visit:

`http://www.pc.ibm.com/ww/eserver/xseries/tape.htm`

Table 9-3 IBM 4560-SLX options

Option	Description	Comment
59P6657	IBM Fibre Channel Card	Require either 59P1271 or 59P1272
59P6658	Ultrium 1 Drive	LVD Connection
59P6659	LTO Cartridge Magazine	Left and Right base magazines
59P6662	Elevator Link	Required when adding a second module
59P6663	Elevator Link Extension	Required when adding two or more modules
59P1271	Longwave GBIC	To be used in conjunction with 59P6657
59P1272	Shortwave GBIC	To be used in conjunction with 59P6657
49P3200	100GB Ultrium 1 Tape cartridge	

Option	Description	Comment
35L2086	Universal LTO Cleaning cartridge	

There are no additional part numbers required for the 3607-26X except the data cartridge 49P3200 and the Universal LTO Cleaning Tape 35L2086.

9.3 Physical attachments

The 4560-SLX Modular Tape Library and 3607-26X Autoloader can be attached to IBM xSeries servers and other Intel/Windows servers that support the SCSI LVD and Fibre Channel interface. Refer to the latest compatibility matrix to determine which xSeries servers support the libraries:

`http://www.pc.ibm.com/us/compat/storage/tmatrix.html`

SCSI cables and appropriate interposers, as required, should be ordered for attachment to a server. A power cord feature code should also be specified.

9.4 Cabling

A SCSI cable is required for each library connection to a SCSI bus. If no cable is available, one should be specified on the initial order for each library or drive. A SCSI terminator is included with each cable. An interposer (a connector that matches the pin pattern of the host adapter to the pin pattern of the cable) may also be required for attachment to particular server adapters.

Be sure to determine the exact SCSI connection type at the host to ensure that the correct cable connections are ordered, then determine the length from the host to the tape library.

The overall LVD SCSI cable length is limited to 25 m (81 feet) using point-to-point interconnection. If using multi-drop interconnection, then the overall LVD SCSI cable length is limited to 12 m (39 feet). The stub length at each device must not exceed 0.1 m (0.33 feet).

For FC cables, there are only two connection types, LC and SC. Once the connection type is determined then only a correct length has to be determined.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1536
Doc: 3690

9.5 Environmental specifications

The physical dimensions for the 4560-SLX are:

- Width: 42.4 cm (16.7 in)
- Depth: 78.7 cm (31 in)
- Height: 22.2 cm (8.75 in) for a stand-alone library on casters
- 5 EIA units high (if rack-mounted)

The physical dimensions for the 3607-26Xare:

- Width: 44.7 cm (17.7 in)
- Depth: 70.3 cm (29.7 in)
- Height: 8.9 cm (3.5 in) for a stand-alone library on casters
- 2 EIA units high (if rack-mounted)

9.6 Storage applications

The software to manage the tape libraries is not provided with the libraries. Additional software support is available through library management software products that must be obtained separately from IBM, IBM Business Partners, or independent software providers. Contact your vendor for information about support of xSeries tape products, or see the IBM ServerProven® Web site at:

`http://www.pc.ibm.com/us/compat/`

9.7 Media

One Ultrium cleaning cartridge and one Ultrium data cartridge are included with each library drive order[1]. With the initial order, additional data and cleaning cartridges may be ordered as a part number.

- Part number 49P3200 provides a single Ultrium 1 Cartridge.
- Part number 35L2086 provides a single Ultrium Cleaning Cartridge.

After the initial order, additional supplies can be ordered from the IBM media business or a third-party media vendor.

`http://www.storage.ibm.com/media/index.html`

Refer to Appendix A, "LTO Ultrium tape media" on page 223, for details about ordering supplies and cartridges, with or without labels.

[1] All media and cleaning cartridges are warranted separately from the IBM 3580 Ultrium tape drive.

9.8 Installation and performance considerations

Installing more than one Ultrium drive on a SCSI bus may affect tape drive performance. For optimal performance, it is recommended that no more than one IBM Ultrium drive be attached to an individual SCSI bus.

While the IBM Ultrium tape drives provide the capability for high tape performance, other components of the system may limit the actual performance achieved. The compression technology used in the tape drive can typically double the amount of data that can be stored on the media; however, the actual degree of compression achieved is highly sensitive to the characteristics of the data being compressed.

9.9 Library features

The following section covers some of the major items required to implement, manage, and operate the IBM tape libraries. It does not cover all tasks and we do not intend to cover all of the specific commands. For more details, refer to the manual for your library listed in Table 9-6, "Library manuals" on page 211.

9.9.1 Identifying library locations element numbers

To manipulate the media within the library, the host must reference each movement with source and target designations. This is done via element addressing, which specifies precisely which slots within the library are to be used. Table 9-4 shows the element addressing scheme used for the 4560-SLX tape library.

Table 9-4 IBM 4560-SLX element numbering

Column	Element numbers
Picker	0
I/O station	448
Drives	480-481
Storage	32-58

Table 9-5 on page 208 shows the element addressing scheme used for the 3607-26X tape library.

ECT
CPMI - CORREIOS
Fls. Nº 1537
Doc: 3690

Table 9-5 IBM 3607-26X element numbering

Column	Element numbers
Picker	0
I/O station	N/A
Drives	32
Storage	256-271

9.10 Operator displays and buttons

Normally, the host issues commands to the tape library. Operator control is provided via the Operator Panel. The operator is responsible for:

- Starting the tape library
- Shutting down the tape library
- Handling media

Refer to the manual for your library, listed in Table 9-6, "Library manuals" on page 211, for your library for media handling procedures. In the case of equipment failures, the operator can perform media processing.

9.10.1 Operator panels

Figure 9-3 and Figure 9-4 on page 209 show the operator panels for the 3607-26X and 4560-SLX respectively.

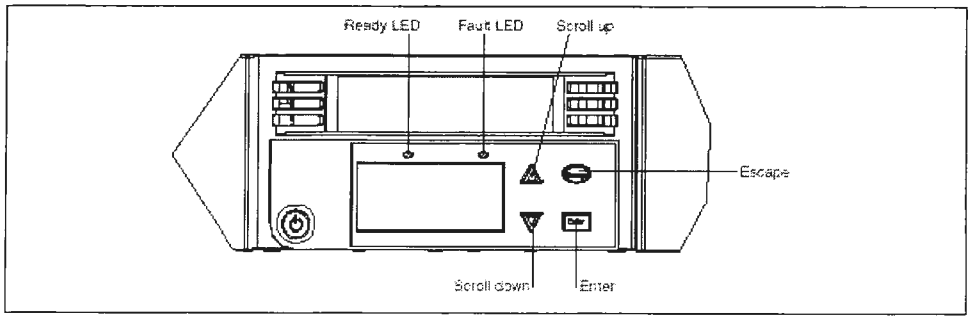


Figure 9-3 3607-26X front panel

Figure 9-4 4560-SLX touch screen front panel

The operator panel provides communication between the operator and the IBM tape library. Visual indications and push buttons enable the operator to control the tape library.

1. I/O Station status:
   The I/O Station status area provides constant information about the I/O Station.
2. Library status:
   The library status area displays information such as online or offline status, library reports status, and messages to solicit operator intervention.
3. Messages:
   The display communicates interactive dialogs, special messages, alerts, and library configurations. More details are covered in the operator manual.
4. Drive status:
   The drive status area provides constant information about the drives, such as:
   - Presence of tape drive (illustrated by a black outline box for each drive)
   - Power to the tape drive
   - Cleaning requirements
   - Compression
   - Write protection
   - Tape activity

RQS nº 03/2005 - CN - CPMI - 1538
Fls. Nº
Doc: 3690

9.10.2 Menu options

Each menu is accessible through the Operator Panel push buttons. For the actual menus for your library, refer to the manual for your library listed in Table 9-6, "Library manuals" on page 211.

Using commands that require an offline state

Some commands require that the library be in an offline state. If any such commands are attempted while the library is in an online state, the operator will be requested to take the library offline.

Operator intervention message

If a problem causes an operator intervention message to appear, refer to the messages section of your operator manual.

9.11 Library modes

The libraries operates in either base or random access mode. The Library Mode will be determined by the application software managing your library.

9.12 Drive cleaning

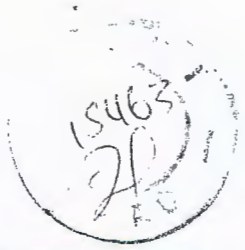
All IBM Ultrium Tape Drives have an integrated cleaning mechanism which brushes the head at load time and again when unloading a cartridge. The drives also have a cleaning procedure that uses a special cleaning cartridge, should this become necessary.

Attention: When cleaning the drive head, use only the IBM LTO Ultrium Cleaning Cartridge or an IBM-approved cleaning cartridge.

With each library, a specially labeled IBM LTO Ultrium Cleaning Cartridge is supplied to clean the drive head. The drive determines and alerts you when the head needs to be cleaned. Refer to the operations manual for details for Automatic Cleaning or Manual Cleaning.

9.13 Firmware upgrades

Each IBM Ultrium tape drive and tape library contains IBM Licensed Internal Code, often referred to as firmware. At installation time, make sure the current



firmware is installed on your IBM LTO tape drives and library. As the libraries are designated as a Customer Setup Machine, it is the customer's responsibility to have the current firmware installed. Determine the latest level of firmware available by visiting `http://www.pc.ibm.com/` or by contacting the IBM Call Center.

Follow the instructions for updating your firmware in the operator manual for your library. Table 9-6 shows the various manuals available for the xSeries LTO products.

Table 9-6 Library manuals

Manuals	Part numbers
1x16 Autoloader Quick Start Guide	71P9131
1x16 Autoloader User's Guide	46P3206
4560SLX Tape Library Quick Installation Guide	59P6702
4560SLX User's Guide	59P6690
Fibre Channel Option Card Users Guide	59P6748

ROS nº 03/2005 - CN - CPMI - CORREIOS
1539
Fls. Nº
Doc: 3690

10

LTO and iSeries considerations

This is a short overview and update about installation and implementation of LTO Tape Drives and LTO Tape Libraries for iSeries.

A redbook and Redpaper address this topic:

- *iSeries in Storage Area Networks,* SG24-6220
- *The LTO Ultrium Primer for IBM @server iSeries Customers*, REDP3580

However, these publications cover only LTO Ulrium 1, so we will provide updates and additional information.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03 2005 - CN - CPMI - CORREIOS
Fls. Nº 1540
Doc: 3690

10.1 iSeries support for IBM LTO Ultrium 2

IBM LTO Ultrium 2 tape drives are supported on RISC machines with OS/400 V5R1 and later.

The following PTFs are needed:

- V5R1 SI07884
- V5R2 SI07885

These PTFs fix a problem with the INZTAPcommand when using LTO 1 and 2 media in the same library.

Tip: *Info APARs*, periodically issued by IBM, contain important information about iSeries topics. There are currently two Info APARs about LTO: II12621 for Ultrium 1 and II13513 for Ultrium 2. These are available in the PTF database, from the Web site:

`https://techsupport.services.ibm.com/server/support?view=iSeries`

Look in the Find it Fast column, and choose Search Technical Databases. Leave the box at the top set at Search APARs, and click **Go**. Enter the Info APAR number in the search box and click **Search**.

You will need these V5R1 and V5R2 PTFs if you change the TAPF from its default density of *DEVTYPE. This is normally only done when using *NL tape label processing.

LTO 2 products can be attached to iSeries systems with any of these adapters:

- 6534 Magnetic Media Controller (SPD), HVD, HD68

  Up to 17 MBps (60 GBph)
- 2729 PCI Magnetic Media Controller, HVD, HD68

  Up to 13 MBps (47 GBph)
- 2749 PCI Ultra Magnetic Media Controller IOA, HVD, HD68

  Up to 38 MBps (108 GBph)
- 5702 Ultra160 SCSI IOA PCI-X Ultra Tape Controller, LVD, VHDCI

  Up to 70 MBps (250 GBph)
- 2765 FC IOAPCI Fibre Channel Tape Controller

  Up to 95MBps (340 GBph)

LTO 2 SCSI drives are supported with multiple drives connected to a single adapter (daisy-chained) for either the LVD or HVD adapters. The LTO 1 drives are still limited to a single-drive configuration.

The following restrictions apply:

- No support for LVD SCSI LTO 1 products on the 5702 adapter
- No 6501 support for LTO 2

There is no performance increase with the HVD SCSI attached LTO 2 devices. Performance is limited by the HVD SCSI interface.

10.2 BRMS and LTO tape libraries

Both LTO 1 and LTO 2 drives can be in the same logical library and share a common inventory *but* you must not attach both drive types to the same I/O adapter. They must be separated at the adapter level for OS/400 to pool the drives together properly.

At the time of writing, OS/400 will show both the LTO 1 (L1 media type) and LTO 2 (L2 media type) as *L* so the user will not be able to determine from the WRKTAPCTG screen which cartridges are of which type.

OS/400 will NOT filter out the LTO 2 cartridges from the LTO 1 MLB so it is up to the user to manage the cartridges using BRMS media classes. The LTO 1 cartridges will have to be added to media class ULTRIUM1, and LTO 2 tapes will have to be added to media class ULTRIUM2. Attempting to use an LTO 2 cartridge in a LTO 1 drive will result in a failure.

For LTO 1 drives the density *CTGTYPE will result in *ULTRIUM1 for LTO 1 cartridges, and the density *DEVTYPE will result in *ULTRIUM1. LTO 2 cartridges are not supported in LTO 1 drives.

For LTO 2 drives the density *CTGTYPE will result in *ULTRIUM1 for LTO-1 cartridges and *ULTRIUM2 for LTO 2 cartridges. The density *DEVTYPE will only work for the LTO 2 drive with LTO 2 media, the device's highest capability.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1541
Doc: 3690

10.3 iSeries resources

The iSeries can control drives and libraries through CL commands and APIs or through software such as BRMS/400. For V4R4 and later, LTO devices report as:

IBM 3580

- 3580 tape drive:
  - Resource -> 3580, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 002

IBM 3581

- 3581 tape drive:
  - Resource -> 3581, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 002
- 3581 Autoloader unit:
  - Resource -> 3581, Device Description -> TAPMLBxx (xx=01, 02, 03, etc.)

When the IBM 3581 is in random mode and an IPL is run for the system or IOP, a TAPMLBxx and TAPxx resource will be created. If the drive is in sequential mode and an IPL is run for the system or IOP, then only a TAPxx resource will be created (that is, the TAPMLBxx will be removed). If the drive normally is used in random mode, it can be changed to sequential mode. In this case, de-allocate the tape resource from the WRKMLBSTS command screen and vary on the tape drive to use as a standalone drive. Make sure the system has not run an IPL before changing the drive back to random mode. If the autoclean function is enabled or disabled, the IOP or IOA must run an IPL before using the 3581 device.

If the barcode feature is installed, the device is in random mode, and the drive is powered up with a cartridge loaded, the loaded cartridge will be missing when a WRKTAPCTG command is run on the iSeries. The cartridge has to be unloaded and the library re-inventoried to show the cartridge. If the 3581 is to be used as an alternate IPL device (as in a D Mode IPL), set the SCSI address on the tape device to 0.

Unloading volumes on IBM 3581

When using the 3581 device in sequential mode, if a user selects the option Load Slot and SRC Slot to mount a volume in the drive (when using tape commands CHKTAP, DSPTAP, INZTAP, SAVxxx, with the ENDOPT(*UNLOAD)), the cartridge will eject from the drive but will not be returned to a slot. For this to happen, the user must specify SEQ START. Loading a slot is a manual operation and the autoloader will not return the cartridge, so it must be unloaded as it was loaded from the panel. The autoloader operation must be *started* to get the cartridges loaded and unloaded.

IBM 3582

- IBM 3582 tape drives:
  - Resource -> 3582, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 002
- IBM 3582 Robotic:
  - Resource -> 3582, Device Description -> TAPMLBxx (xx=01, 02, 03, etc.)
  - 3582 023 with 3580 002 drives

IBM 3583

- IBM 3583 tape drives:
  - Resource -> 3583, Device Description -> TAPxx (xx=01, 02, 03, etc.)
  - 3580 001 and 3580 002
- IBM 3583 Robotic:
  - Resource -> 3583, Device Description -> TAPMLBxx (xx=01, 02, 03, etc.)
  - 3583 0xx with 3580 001 and 3580 002

3583 with SDG Fibre Channel limitations

The 3583 device with FC 8005 (Fibre Channel attach) uses only LVD SCSI drives. V5R1 and later have Fibre Channel support. All FC attachments must be direct attached or homogeneous zones with iSeries only. The 3583 FC attached library has two Fibre Channel ports. The device can be shared with other platforms but it is strongly recommended that each platform be connected to separate ports. If zoning is used in the SAN device, be sure that the all iSeries hosts have a connection to the media changer. All six tape devices can be used but performance must be considered with the larger configuration. Alternate IPL is not supported for Fibre Channel attached tape devices. The Alternate Install Device (Boot Manager) must be used instead.

3583 non-multi-path architecture Fibre Channel recommendations

When sharing the 3583 FC with two or more hosts concurrently it may fail if the default time out for the *initial mount wait time* and the *EOV mount wait time* is used. These values have to be increased to a suggested 5-10 minutes. In general, larger library configurations and shared configurations tend to get a time-out error, so increasing this value is required.

IBM 3584

- IBM 3584 Tape drives:
  - Resource -> 3584, Device Description -> TAPxx (xx=01, 02, 03 etc.)
- IBM 3584 Robotic:
  - Resource -> 3584, Device Description -> TAPMLBxx (xx=01, 02, 03 etc.)
  - 3584 032 with 3580 001 and 3580 002 drives

Note: The Problem Analysis Log (PAL) will show 63A0 and 9429.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1542
Doc: 3690

Fibre Channel limitations

For V5R1, the iSeries Fibre Channel 3584 support is limited to a single-drive configuration per adapter. Multiple systems may share a drive with the use of a 3534 Hub or 2109 switch. If the 2109 switch is used it must be set to Quick Loop mode for the ports used on the iSeries. Each system or LPAR may have multiple drives but each drive requires an adapter. Each drive connection must have a library control path enabled.

Alternate IPL is not supported for Fibre Channel attached tape devices.The Alternate Install Device (Boot Manager) must be used instead.

10.3.1 Configuration changes

If making any configuration changes on LTO drives and libraries you must run an IPL on the IOA/IOP on the iSeries.

10.4 OS/400 V5R1 restriction for multi-path architecture libraries

The IBM 3582, 3583, and 3584 feature multi-path architecture. Unlike other platforms, the iSeries requires a dedicated control path for each iSeries drive. This is true for both SCSI and fibre drives for OS/400 V5R1. This is not the way the library is shipped, so you have to enable the control paths on all drives that are connected to an iSeries. You can do this either on the operator panel or with StorWatch. If you forget to do this, the drives will not autoconfig properly.

If you have configured your library properly, then you will see as many tape libraries in OS/400 as there are tape drives are assigned to your server. For example, if you have a 3584 with three drives assigned to the iSeries, then you see three TAPMLBxx (TAPMLB01, TAPMLB02, TAPMLB03), each with three TAPxx (TAP01, TAP02, TAP03).

10.5 OS/400 V5R2

Version 5 Release 2 includes support for multiple targets from a single Fibre Channel tape or disk adapter. Before this release, only a single target was supported from an initiator (FC adapter). Up to 16 LUNs are supported. A target is a physical tape drive. In the case of tape this means a single-tape FC adapter can support multiple tape devices. For example, with V5R1, if you had four iSeries with four FC tape devices, sixteen FC tape adapters would have been required to enable all iSeries to address all tape devices, as each FC adapter is

allowed to see only one target. At V5R2 this number is reduced to four, one FC tape adapter per iSeries because each FC adapter may see multiple targets. This is illustrated in Figure 10-1. In summary, LTO 2 and V5R2 FC allow multiple device configurations per adapter and therefore one control path per adapter is required.

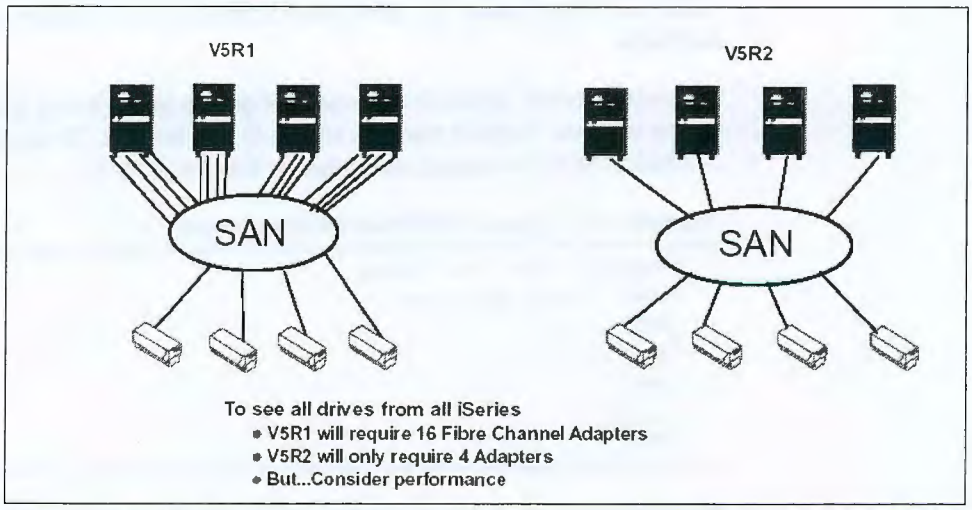


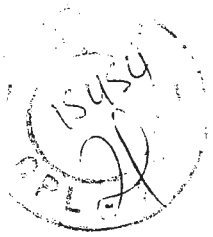
Figure 10-1 Multiple-target support

A maximum of 16 tape LUNs may be addressed from a single iSeries tape FC adapter. A LUN is a tape device or media changer. So in the case of a 3583 LTO tape library, which may have six drives and a media changer, seven LUNs will be reported. This example dramatically decreases the cost of hardware required to support multiple devices from multiple iSeries, but there are other considerations, such as management of tape devices.

Sharing the devices requires only a standard **`vary on`** and **`vary off`** command. When the iSeries varies on a tape it will use a *reserve* lock on the tape device to prevent other systems from using the drive. However, in a heterogeneous setup other operating systems may also share the drive. A benefit of the iSeries is its ability to *reserve/release* a tape drive. This prevents other systems writing to the middle of a tape in use by an iSeries and ensures tape data integrity for iSeries users. The same may not be true for other operating systems, and therefore it is entirely possible for an iSeries to start using a tape drive in use by another system. You will have to check with each vendor to establish whether they support *reserve/release* of a tape drive.

Tape management software such as BRMS and IBM Tivoli Storage Manager use the *reserve* lock. For other packages, check with the software vendor.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1543
Doc: 3690



10.6 Tape drive sharing and management

OS/400 is an integrated operating system, so all device management function is included, with no extra software required for drive allocation and automation. This function simplifies drive sharing, especially when fibre drives are used, and all hosts can see all drives. This section shows how it works; it is the same for both SCSI and fibre drives, but using fibre drives is more flexible, as more drives are available.

On each system, OS/400 will autoconfigure a tape library, and will find all of the drives that are inside it that are visible to the system. To see this, use the WRKMLBSTS command, as shown in Example 10-1.

Example 10-1 Output of WRKMLBSTS command

```
TAPMLB01  <<<<< the library
TAP01   <<<<< the drives
TAP02
TAP03
TAP04
 .....
TAPxx
```

For each drive you have to set the options that are at the top of the WRKMLBSTS command screen. You have three options:

- ALLOCATED: means that ONLY the system where it is allocated can use it.
- DEALLOCATED: means the system you are looking on CANNOT use it.
- UNPROTECTED: means that the drive will sit in limbo waiting for a system to use it. That system will use it, then put it back into *limbo* ready for the next system to use it.

For drive sharing, you would set all drives to UNPROTECTED status. This is the most common setup, especially on fibre.

When backing up with BRMS, just tell BRMS to save to TAPMLB01. BRMS will find a tape, find a drive, and run the save. If doing parallel saves, BRMS will get multiple drives running at once. You can also submit multiple jobs to get multiple drives running at once. And if all of the drives are busy and you submit another job, OS/400 will hold the new job on the library manager resource queue until a drive becomes available. Note that in order for this to work well, you will need to use CHGDEVMLB to increase the timeout parameters on the Initial Volume Mount Wait and End of Volume Mount Wait times. The defaults are 10 minutes, whereas 8 hours or similar is recommended for Initial Volume Mount Wait. If you have some saves that are higher priority than others, you may want to adjust the order you start them up, to make sure the critical ones get the drives first. If you

make a mistake, then within each system, OS/400 will prioritize the jobs on the library manager resource queue, and at the next tape mount, it will swap out the job that was running, and move in the job with the higher tape resource priority.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1544
Doc: 3690

LTO Ultrium tape media

When an IBM 35XX Ultrium tape device is ordered, it will be supplied with one Ultrium data cartridge and one cleaning cartridge at no charge. Each member of the IBM 35XX Ultrium LTO family has different media features and rules that apply when placing the order. The following informationwill assist you in ordering additional media.

You can obtain tape cartridge supplies for use with the IBM LTO Ultrium 1 product family in three ways:

- Order features from IBM that are available only with the initial hardware order as described in "Features available with IBM LTO hardware initial order" on page 225.
- Order the IBM LTO Ultrium 1 media product offering (using a dummy IBM model type, 3589) as described in "IBM 3589 Ultrium 1 tape cartridge model number" on page 228.
- Contact the IBM MEDIA business supplies or a third-party supplier as described in "IBM media business distributors and other suppliers" on page 231.

You can obtain tape cartridge supplies for use with the IBM LTO Ultrium 2 product family in two ways:

- Order features from IBM that are available only with the initial hardware order as described in "Features available with IBM LTO hardware initial order" on page 225.

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1545
Doc: 3690

- Contact the IBM MEDIA business suppliers or third-party suppliers as described in "IBM media business distributors and other suppliers" on page 231.

Each of the following *additional media* features for Ultrium 2 will supply data cartridges with barcode labels that are not fixed to the data cartridges. The barcode labels will have be physically attached and the actual value of barcode labels cannot be pre-determined. For cartridges with fixed barcode labels and pre-determined barcode values, it is recommended that the media always be ordered through 1-800-IBM-MEDIA (refer to "IBM media business distributors and other suppliers" on page 231).

The media suppliers may supply tape cartridges from different manufacturers or offer a choice of brands. The tape cartridges you use must be manufactured by a qualified LTO media company to meet the LTO standards.

Features available with IBM LTO hardware initial order

The following media features are available for inclusion with the initial hardware order.

IBM TotalStorage Ultrium 1 Tape Drive 3580

These chargeable features provide media with the IBM 3580 Ultrium 1 tape drive and are available only with the initial order:

- Feature #8001 provides a single 100 MB Ultrium data cartridge with an unattached barcode label.

  A maximum of five is allowed.

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of three is allowed.

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with a barcode are included as standard with each initial order[1].

IBM TotalStorage Ultrium 2 Tape Drive 3580

These chargeable features provide media with the IBM 3580 Ultrium 2 tape drive and are available only with the initial order:

- Feature #8101 provides a single 200 MB Ultrium data cartridge without an attached barcode label.

  A maximum of 20 is allowed.

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of five is allowed.

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with a barcode are included as standard with each initial order.

IBM TotalStorage Ultrium Tape Library 3582

These chargeable features provide media with the IBM 3582 tape library and are available only with the initial order:

- Feature #8001 provides a single 100 MB Ultrium data cartridge.

  A maximum of 19 is allowed.

[1] Note that all media and cleaning cartridges are warranted separately from the IBM 3580 tape drive hardware.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1546
Doc: 3690

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of three is allowed.

- Feature #8110 provides a pack of twenty 100 MB Ultrium data cartridges with unattached barcode labels.

IBM TotalStorage Ultrium 1 Scalable Tape Library 3583

These chargeable features provide media with the IBM 3583 Ultrium 1 tape library and are available only with the initial order:

- Feature #8001 provides a single 100 MB Ultrium data cartridge.

  A maximum of 19 is allowed.

- Feature #8002 provides a single Ultrium cleaning cartridge.

  A maximum of three is allowed.

- Feature #8010 provides a pack of twenty 100 MB Ultrium data cartridges with unattached barcode labels.

  The maximum allowed for different model types is shown in Table A-1.

Table A-1 Maximum number of media features for IBM 3583 Ultrium 1

IBM 3583 model	#8007 (cartridge cells)	#8010 (maximum allowed)
L18	0	1
L18	1	2
L18	2	3
L36	0	2
L36	1	3
L72	not applicable	4

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with barcode are included as standard with each initial order[2]

[2] Note that all media and cleaning cartridges are warranted separately from the IBM Ultrium hardware.

IBM TotalStorage Ultrium 2 Scalable Tape Library 3583

These chargeable features provide media with the IBM 3583 Ultrium 2 tape library and are available only with the initial order:

- Feature #8101 provides a single 200 MB Ultrium data cartridge without barcodes.

  A maximum of 19 is allowed.

- Feature #8110 provides a pack of twenty 200 MB Ultrium data cartridges without barcodes.

  The maximum allowed for different model types is shown in Table A-2.

Table A-2 Maximum number of media features for IBM 3583 Ultrium 2

IBM 3583 model	#8007 (cartridge cells)	#8110 (maximum allowed)
L18	0	4
L18	1	4
L18	2	4
L36	0	4
L36	1	4
L72	not applicable	4

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge without barcodes are included as standard with each initial order.

IBM TotalStorage Ultrium 1 UltraScalable Tape Library 3584

These chargeable features provide media with the IBM 3584 Ultrium 1 tape library frame models and are available only with the initial order:

- Feature #8750 provides a single Ultrium cleaning cartridge.

  A maximum of 10 is allowed.

- Feature #8757 provides a pack of twenty 200 MB Ultrium data cartridges without barcodes.

  The maximum allowed for different model types is shown in Table A-3 on page 228.

CPMI - CORREIOS
Fls. Nº 1547
Doc: 3690

Table A-3 Maximum number of media features for IBM 3584 Ultrium 1

IBM 3584 model type	#1603 (capacity expansion)	#8757 (maximum allowed)
L32 (base)	0	1
L32 (base)	1	1
D32 (expansion)	not applicable	1

In addition to these features, one Ultrium cleaning cartridge and one Ultrium data cartridge with barcode are included as standard with each initial Model L32 library order[2].

IBM TotalStorage Ultrium 2 UltraScalable Tape Library 3584

These chargeable features provide media with the IBM 3584 Ultrium 2 tape library frame models and are available only with the initial order:

- Feature #8767 provides a pack of twenty 200 MB Ultrium data cartridges without barcodes.

  The maximum allowed for different model types is shown in Table A-4.

Table A-4 Maximum number of media features for IBM 3584 Ultrium 2

IBM 3584 model type	#1603 (capacity expansion)	#8757 (maximum allowed)
L32 (base)	0	1
L32 (base)	1	1
D32 (expansion)	not applicable	1

IBM 3589 Ultrium 1 tape cartridge model number

You can use the IBM 3589 model number to order quantities of IBM LTO Ultrium 1 data and cleaning cartridges. Since this is not a true hardware machine type, engineering installation and maintenance are not relevant to it, no real serial number is applied to it (although cartridges have their own serial number types), and no MES features can be added to it once delivered.

Note there is no 3589 equivalent for Ultrium 2 tape cartridges.

Model description

You may choose from three model types for the IBM 3589, where each model delivers a different cartridge specification:

- IBM 3589-004 provides Ultrium cleaning cartridges.

  Model 004 has a single chargeable feature, #4005, which indicates the required quantity of cleaning cartridges. Each feature delivers a pack of five cleaning cartridges. You must order at least one of these features for this model.

  The maximum allowed is six features per model order for a total of 30 cartridges; if you require more than 30 cartridges, order a second 3589 model 004 with additional features.

- IBM 3589-003 provides Ultrium 1 data cartridges with no labels.

  Model 003 has a single chargeable feature, #3020, which indicates the required quantity of unlabeled data cartridges. Each feature delivers a pack of 20 data cartridges. You must order at least one of these features for this model.

  The maximum allowed is 20 features per model order (400 cartridges); if you require more than 400, order a second model 003 with additional features.

- IBM 3589-002 provides Ultrium 1 data cartridges with a labeling service.

  Model 002 has a single chargeable feature, #2020, which indicates the required quantity of labeled data cartridges. As with the model 003, each feature delivers a pack of 20 data cartridges, and you must order at least one of these features for this model with a maximum of 20 features per model.

  However, in addition, you must order various no-charge features to indicate what volume serial range you want printed on the cartridge labels. The supplied barcode label is made up of 8 characters, a six-character VOLSER, and a two-character cartridge media-type identifier (L1), which identifies the cartridge as an LTO cartridge (L) and indicates that the cartridge is the first generation of its type (1). The format of the VOLSER is explained in 2.3.4, "Volume label format" on page 23.

Labelling service

This service applies only to the IBM 3589 model 002.

There are six characters in the VOLSER, and IBM provides specific codes to allow you the flexibility to choose where to begin the volume range you require. The sixth character is always zero as your volume serial range must always begin at a 0 boundary for labeling, and the labels supplied are sequential. So, for

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1548
Doc: 3690

example, if you order 20 cartridges the first cartridge will be labeled with a sixth digit of 0, and the twentieth cartridge will be labelled with a sixth digit of 9.

The character identifier features are four-digit feature numbers of the form 9nnn, composed as follows:

- The first digit 9 means the feature carries no charge.
- A second digit of 1, 2, 3, 4, or 5 indicates which character in the VOLSER this feature is specifying (1st, 2nd, 3rd, 4th, or 5th).
- The third and fourth digits range from 00 through 35, where 00 through 09 represent the characters 1 through 9, and 10 through 35 represent the characters A through Z.

Choose the first 1, 2, 3, 4, or 5 digits by using the feature numbers as follows:

- First alphanumeric digit (0 to 9 or A to Z): use #9100 (0) to #9135 (Z).
- Second alphanumeric digit (0 to 9 or A to Z): use #9200 (0) to #9235 (Z).
- Third alphanumeric digit (0 to 9 or A to Z): #9300 (0) to #9335 (Z).
- Fourth numeric digit (0 to 9): use #9400 (0) to #9409 (9).
- Fifth numeric digit (0 to 9): use #9500 (0) to #9509 (9).
- Sixth numeric digit is set to 0 as standard.
- Seventh character of Volser is set to L.
- Eighth character of Volser is set to 1.

If you do not specify a feature number then the supplied starting character will be zero. Thus if you specify features for the first thee characters as ABC but no more, then the sequence of labels will begin ABC000.

Two specific features indicate requirements for colored labels:

- Feature #9077 specifies a white background.
- Feature #9022 specifies a colored background for the alpha characters.

If you specify #9022, then you can choose from 10 available colors shown in Table A-5 on page 231.

Table A-5 Color specify feature codes for the IBM 3589 model 002

Alpha prefix background	Feature code	Alpha prefix background	Feature code
red	9003	orange	9008
yellow	9004	pink	9009
light green	9005	dark green	9010
light blue	9006	light orange	9011
gray	9007	purple	9012

IBM media business distributors and other suppliers

If you want to buy additional supplies for the IBM LTO Ultrium product families you can obtain them from the IBM media business suppliers or third-party suppliers. To purchase in this way you must quote the Ultrium part numbers (not feature numbers or model types) for the different items required. The part numbers are listed in Table A-6.

Table A-6 LTO Ultrium 1 and 2 available supplies and part numbers

Part number	Description
08L9120	IBM LTO Ultrium 1 data cartridge
08L9870	IBM LTO Ultrium 2 data cartridge (no barcode label)
19P5887	IBM LTO Ultrium 2 data cartridge (with barcode label)
35L2086	IBM LTO Ultrium cleaning cartridge
08L9129	Leader pin attachment kit
08L9130	Cartridge rewind tool
13F5647	IBM tape unit cleaner
2108930	Lint-free cloth

To obtain these supplies or for warranty replacements, use the appropriate distributor for your country location:

- United States and Canada:
  For information about Priority Fulfillment Services distribution channels call 1-888-IBM-MEDIA in the U.S. and Canada.

- Latin America:
  For information about Priority Fulfillment Services distribution channels call +1-972-881-0733.
- Asia Pacific:
  For information about Priority Fulfillment Services distribution channels call +81-3-3808-8486 in Japan or +1-972-881-0733 outside of Japan.
- Europe, Middle-East, and Africa:
  For information about Priority Fulfillment Services Europe distribution channels call +31-433-502-756.
- Other country-specific numbers can be found at:

  `http://www.storage.ibm.com/media/lto/index.html`

Abbreviations and acronyms

AC	Alternating Current
AIM	Automatic Identification Manufacturers
AIT	Advanced Intelligent Tape
AIX	Advanced Interactive Executive
ALDC	Adaptive Lossless Data Compression
AME	Advanced Metal Evaporative
AMP	Advanced Metal Evaporative
ANSI	American National Standards Institute
API	Application Programming Interface
ATF	Auto Tracking Following
BRMS	Business Recovery and Management Services
CM	Cartridge Memory
CRC	Cyclic Redundancy Check
CVE	Compliance Verification Entity
DAT	Digital Audio Tape
DC	Direct Current
DDS	Digital Data Standard
DLT	Digital Linear Tape
ECC	Error checking and correction
ECMA	European Computer Manufacturer's Association
EEPROM	Electrically Erasable Programmable Read-Only Memory
EOT	End of tape
EOV	End of volume
ESCON	Enterprise Systems Connection
FC	Fibre channel/feature code
FC-AL	Fibre channel arbitrated loop
FCP	Fibre channel protocol
FICON	Fiber Connectivity
FRU	Field replacable unit
HBA	Host bus adapter
HSM	Hierarchical storage management
HVD	High voltage differential
IBM	International Business Machines
IDRC	Improved Data Recording Capability
IOP	Input/output processor
ISV	Industry solution provider
ITSO	International Technical Support Organization
LAN	Local area network

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1550
3690
Doc:

LGMR	Laser Guided Magnetic Recording
LIP	Loop initialization protocol
LPAR	Logical partition
LPOS	Longitudinal Positioning
LTO	Linear Tape Open
LTO-CM	Linear Tape Open-cartridge memory
LTO-DC	Linear Tape Open Data Cartridge
LUN	Logical unit number
LVD	Low voltage differential
MCC	Medium changer controller
MES	Machine equipment specification
MFM	Modified Frequency Modulation
MIB	Management information block
MRC	Magneto-Resistive Cluster
MTBF	Mean time between failures
OEM	Original equipment manufacture
P/N	Part number
PCBA	Printed circuit board assembly
PCI	PC Connect interface
POS	Pivoting Optical Servo
PRML	Partial Response Maximum Likelihood
PTF	Program temporary fix
QIC	Quarter inch cartridge
RF	Radio frequency
RLL	Run Length Limited
RMU	Remote Management Unit
SAN	Storage Area Network
SARS	Statistical Analysis and Reporting System
SCSI	Small computer systems interface
SDG	SAN Data Gateway
SDLT	SuperDLT
SLDC	Streaming lossless data compression
SMIT	Systems Management Interface Tool
SNIA	Storage Networking Industry Association
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
VHDCI	Very High Density Cable Interconnect
VPD	Vital Product Data
WWN	World Wide Name

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see "How to get IBM Redbooks" on page 237. Note that some of the documents referenced here may be available in softcopy only.

- *Storage Area Networks: Tape Future in Fabrics*, SG24-5474
- *Designing an IBM Storage Area Network*, SG24-5758
- *Using IBM LTO Ultrium with Open Systems, SG24-6502*
- *Implementing IBM LTO in Linux and Windows*, SG24-6268
- *IBM Tivoli Storage Manager Version 5.1 Technical Guide*, SG24-6554

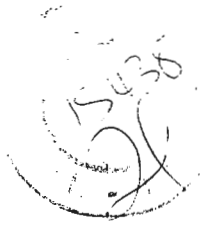
Other publications

These publications are also relevant as further information sources:

- *IBM TotalStorage Tape Device Drivers Installation and User's Guide*, GC35-0154
- *IBM TotalStorage Tape Device Drivers Programming Reference*, GC35-0346
- *IBM Ultrium Device Drivers Installation and User's Guide*, GA32-0430
- *IBM 3580 Ultrium Tape Drive Setup, Operator, and Service Guide*, GA32-0415
- *IBM 3581 Ultrium Tape Autoloader Setup, Operator, and Service Guide*, GA32-0412
- *IBM 3582 Ultrium Tape Library Setup, Operator, and Service Guide*, GA32-0548
- *IBM 3583 Ultrium Scalable Tape Library Setup and Operator Guide*, GA32-0411
- *IBM 3584 UltraScalable Tape Library Planning and Operator Guide*, GA32-0408

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1551
Doc: 3690



Online resources

These Web sites and URLs are also relevant as further information sources:

- This is the main Web site for information about IBM LTO products:

  `http://www.ibm.com/storage/lto`

- The Linear Tape Open Technology Organization Web site provides information about the technology, formats and licensing:

  `http://www.lto-technology.com/`

- The SCSI Trade Association Web site provides information about SCSI standards and terms:

  `http://www.scsita.org`

- This Web site describes the media available from IBM:

  `http://www.ibm.com/storage/media`

- This Web site describes IBM Microelectronics products including compression devices:

  `http://www.chips.ibm.com`

- This Web site describes the Streaming Lossless Compression Algorithm:

  `http://www.ecma-international.org/publications/standards/ECMA-321.HTM`

- IBM Tivoli Storage Manager SAN device support:

  `http://www-3.ibm.com/software/tivoli/products/storage-mgr-san/platforms.html`

- Ultrium device driver downloads:

  `ftp://ftp.software.ibm.com/storage/devdrvr`

- LTO devices update drive firmware:

  `http://ssddom02.storage.ibm.com/techsup/webnav.nsf/support/ltofaqs_updatefw_drivefw`

- ISV Support Matrix for LTO:

  `http://www.storage.ibm.com/hardsoft/tape/conntrix/pdf/lto_isv_matrix.pdf`

- Ultrium 3580 Drive firmware information:

  `http://www-1.ibm.com/support/docview.wss?rs=543&org=ssg&doc=S4000055&loc=en-us`

- IBM 3582 Interoperability Matrix:

  `http://www.storage.ibm.com/tape/lto/3582/3582opn.pdf`

- IBM 3583 Interoperability Matrix:

  `http://www.storage.ibm.com/tape/lto/3583/3583opn.pdf`

- IBM 3584 Interoperability Matrix:

  http://www.storage.ibm.com/tape/lto/3584/3584opn.pdf
- IBM 3584 drive and library firmware:

  ftp://ftp.software.ibm.com/storage/358x/3584
- IBM HBA and SAN Interoperability Matrix:

  http://ssddom02.storage.ibm.com/hba/hba_support.pdf
- IBM Sales Manual:

  http://www.ibmlink.ibm.com/ussman
- IBM ServerProven compatibility for hardware, applications, and middleware:

  http://www.pc.ibm.com/us/compat
- IBM xSeries tape storage:

  http://www.pc.ibm.com/ww/eserver/xseries/tape.html
- IBM iSeries technical support:

  https://techsupport.services.ibm.com/server/support?view=iSeries

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

ROS nº 03/005237 - UN - CPMI - CORREIOS
Fls. Nº 1552
Doc: 3690

Index

Numerics

3580 see IBM 3580
3581 see IBM 3581
3582 see IBM 3582
3583 see IBM 3583
3584 see IBM 3584
8 mm tape 56
9210 121
9211 122
9212 122
9400 122
9600 122

A

activity status display 197
Advanced Metal Evaporative media 51
AIT 57
AIX commands
  cfgmgr 176
ALDC 16–17
arbitrated loop 33
archive life 25
Atape driver 176
autoloader 67
automated tape libraries 68
availability features 41

B

backup 17
bands 6, 10
bands See also servo tracks
barcode
  format 22
barcode label 19
barcode label format 22
barcode reader 117, 132, 202
brick 28

C

call-home 179
capacity 18
capacity, calculation for IBM 3584 185
cartridge door 19
cartridge handling 25
cartridge inspection 27
cartridge life 24
cartridge memory 7, 20, 42
cartridge shipping 26
cartridge slot columns 181
cfgmgr 176
channel calibration 38
cleaning 43, 90, 111, 210
  IBM 3580 91
  IBM 3582 128
  IBM 3583 156
cleaning cartridge 25, 43
codewords 17
coercivity 20
common subassembly 28
compression 16
compression scheme swapping 30
control path 46
control path failover 47, 175

D

DAT 54
data bands 6, 13
data compression 16, 30
data rate 28, 50
  burst 35–36
data tracks
  number of 16
DDS 54
diagnostic cartridge 182
differential SCSI 32
Digital Audio Tape 54
Digital Data Standard 54
Digital Linear Tape 58
direction buffer 16
disaster recovery 74
DLT 58
DLT 2000 60
DLT 4000 60
DLT 7000 61
DLT 8000 61

© Copyright IBM Corp. 2000, 2003. All rights reserved.

RCS nº 03 2005 - CN - CPMI - CORREIOS
Fls. Nº 1553
Doc: 3690

dual-gripper 174
dynamic speed matching 37

E

EEPROM 20
element addresses 194, 196
element numbers 105, 194
enterprise tape libraries 68
error correction 7, 41

F

fast locate function 21
FCA 169, 175, 191
FC-AL 33
Feature
  1603 188
  7003 100
  7004 100
  8001 225
  8002 225
  8003 132, 137
  8004 132, 137
  8006 142
  8008 142
  8012 141
  8105 132
  9022 230
  9077 230
  9210 143, 192
  9211 143, 192
  9212 143, 192
  9213 143, 192
  9215 143
  9400 143, 192
  9600 143, 192
Fibre channel 33
  native 33
firmware 112, 179
  IBM 3580 91
flat lap head 42
frame controller assembly see FCA

G

grips 19

H

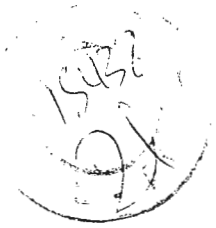
HD68 34
helical-scan recording 50
HVD 80, 95, 115, 132

I

I/O station 185
IBM 113
IBM 3480 63
IBM 3490E 63
IBM 3494 161
IBM 3580 45, 79
  application software support 86
  cartridges 87, 123, 206
  device driver 84–85
  display 89
  feature codes summary 81
  firmware 91
  implementation 87
  interposer 83
  L11 80
  media 87
  Model H11 80
  Model H23 80
  Model L11 80
  operating modes 110
  SCSI adapters 82
  SCSI cables 82
  SCSI ID 87
  SCSI length limitations 83
  server attachments 84
  status light 88
  Storage Applications 86
  unload 90
  upgrade 84
  warranty 81
IBM 3581 45, 93
  access mode 96
  activity bar 107
  barcode reader 98
  cartridge I/O 97
  cleaning 111
  control buttons 108
  device driver 102
  drive status 107
  error code 107
  feature codes summary 96
  general information 95
  Initial setup 104
  interposer 99

library modes 96, 110
media 87, 103
media cartridges 103
message display panel 106
Model H17 95
Model L17 95
operator display 105
optional bar code reader 100
performance considerations 86, 103
SCSI adapter 98
SCSI cables 98
SCSI devices 97
setting SCSI addresses 104
status light 105
storage applications 103
warranty 96
IBM 3582 45, 113
application software support 123
barcode reader 117
capacity 114
cleaning 128
device driver 122
element addresses 125
feature codes summary 118
firmware 128
general information 114
I/O station 117
implementation 124
interposer 121, 140
inventory 117
inventory update 117
library control unit 117
library modes 128
magazines 115
maintenance 118
media 87, 123
model description 114
multi-path architecture 114, 124
operator panel 118, 125–126
performance considerations 124
robotic system 117
SCSI cabling 120
SCSI defaults 125
storage slots 115
IBM 3583 45, 129
cabling options 138
capacity 130
cartridge magazines 133
cleaning 156
control path 135
device driver 144
drive status 152, 209
element addresses 150
feature codes summary 136
firmware 157
general information 130
I/O station 133, 141
implementation 146
inventory 132–133
inventory update 132
library control unit 133
library mode 156
library status 151
magazines 132
maintenance 135
media 87, 145
menu options 127, 153
message display 151
Model L18 131
Model L36 131
Model L72 131
operator panel 134, 151
performance considerations 145
physical library layout 147
redundant power 142
Remote Management Unit 151, 154
RMU 151, 154
robotic system 133
SAN Data Gateway 135
SCSI adapters 137
SCSI defaults 147
SCSI ID and LUN assignment 146
SDG 135
storage columns 132
upgrade 131, 141
IBM 3584 45, 159
accessor 172
bandwidth 187
barcode reader 162, 174
bulk-loading 162
calibration sensor 174
call-home 179
capacity 160, 181
capacity calculation 185
Capacity Expansion feature 162
cartridge gripper 173
cartridge slots 163, 181
components 165

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1554
Doc: 3690



configuration 180
control path 194
control path failover 175
D32 frame 183
device drivers 192
diagnostic cartridge 182
distributed control system 167, 170
drive features 166
Dual AC Power 191
dual-gripper 174
element addresses 194, 196
element numbers 194
expansion frame 161, 188, 196
features 188
firmware 179
floor requirements 190
Frame Control Assembly Feature 163
general information 160
I/O station 162, 177, 185
implementation 194
inventory 186
inventory time 188
library control system 167
logical address 196
LTO Ultrium drives 166
major components 165
media 87
mode of operation 198
Model D32 161, 163, 188
Model L32 161, 181
multi-path architecture 134, 194
operating environment 191
operator display 196
operator panel 171
performance 186
physical address 196
physical dimensions 189
pivot assembly 173
power and cooling 191
rail assembly 174
reliability 177
remote support 179
Remote Support Attachment 179
Remote Support Switch 179
SNMP see SNMP
StorWatch Specialist 176
tape drive element numbers 195
tape drives 162
upgrade options 188
upgrades 188
Vital Library Data 178
Vital Product Data 198
WWN 174
IBM 3607-26X 199
barcode reader 202
capacity 200
element addresses 207
feature codes 205
firmware 210
general information 200
I/O station 202
inventory 202
library manuals 211
library mode 210
media 206
menu options 210
operator panel 208
physical dimensions 206
IBM 4560-SLX 199, 208
barcode reader 202
capacity 201
element addresses 207
Elevator Link Extension Option 201
Elevator Link Option 201
feature codes summary 204
firmware 210
general information 201
I/O station 202
inventory 202
library manuals 211
library mode 210
media 206
menu options 210
operator panel 208
physical dimensions 206
IBM Magstar 3590 64
IBM TotalStorage Enterprise Automated Library 3494 161
IBM TotalStorage UltraScalable Tape Library 3584 see IBM 3584
IBM TotalStorage Ultrium Tape Autoloader 3581 see IBM 3581
IBM TotalStorage Ultrium Tape Drive 3580 see IBM 3580
IBM TotalStorage Ultrium Tape Library 3582 see IBM 3582
IBM TotalStorage Ultrium Tape Library 3582 see IBM 3582

implementation 104, 124, 207
IBM 3580 87
input/output station 162, 177
integrated cleaning mechanism 90
interchangeability of drives 45
interfaces 31
interleaved recording 10
inventory 117, 132, 202

L
label area 19
labelling 229
leader pin 19
library centric WWN 175
Library Control Unit 203
library partitioning 47
library sharing 46, 134
library upgrade 45
linear recording 6, 50
Linear Tape Open
see LTO
load-to-ready time 35–36
locking mechanism 19
logical library 134
longitudinal positioning 12
LPOS 13
LTO 1
barcode 22
cartridge life 24
cartridge memory 20
cleaning cartridge 25
data compression 30
formats 2
interfaces 31
inter-generation compatibility 39
license packages 4
licensing 3
media identifier 23
power supply 28
reliability and availability 41
shelf life 21
specifications 3
LTO 2
performance 36
LTO-CM 20, 24
data fields 21
LTO-DC 16
LVD 80, 95, 115, 132

M
magazine numbering 148
magazines 132–133
Magstar 64
maintenance 204
Mammoth 57
Management Information Base see MIB
MCP
media 223, 225
suppliers 231
media compatibility 20
media labelling 229
Media sharing 72
medium changer pack see MCP
metal particle media 20, 51
MIB 180
multi-path architecture 46, 114, 124, 134, 194
multiple filemarks 38

N
NetView 180
notches 19

O
offsite vaulting 74
operating modes 110
operator interface 170
operator panel 118, 134, 204, 208

P
Partial Response Maximum Likelihood 36
PAUSE 197
performance
load-to-ready 35–36
search time 35–36
unload time 35–36
physical address 195
Pivoting Optical Servo 62
POST 179
power management 38
Power On Self Test see POST
power supply 28

Q
QIC 52
QIC standards 54
quarter-inch cartridge 52

RQS nº 03 2005 - CN -
CPMI - CORREIOS
Fls. Nº 1555
Doc: 3690

R

random access mode 110
RAS 41, 177
  IBM 3584 177
read/verify elements 16, 29
recording format 6
Redbooks Web site 237
  Contact us xxii
Remote Management Unit 134
remote support 179
Remote Support Attachment 179
Remote Support Switch 179
RMU 134
robotic control 203

S

SAN 68
  Loop 71
  Point-to-point 71
  Server to server 69
  Server to storage 69
  Storage to storage 69
  Switched 71
SAN topologies 71
SARS 21, 42
scheme swap 17
SCSI 31
  adapter 82
  address for autoloader 97
  autoloader address 125
  cabling 205
  element address 196
  element numbers 105
  HVD differential 32
  LVD differential 32
  single ended 32
SCSI ID 87
SDLT 62
search time 35–36
sequential access mode 110
serpentine linear recording 51
serpentine recording format 28
Server-free backup 76
servo
  timing based 7
servo bands 11
servo bursts 11
servo elements 30
servo tracks 10, 20, 51
shelf life 25
SNMP 180
  MIB 180
Sony AIT 57
speed matching 37
Statistical 42
Statistical Analysis and Reporting System
  see SARS
status LED 39
STK 9840 65
StorWatch 176
SuperDLT 62
Surface Control Guiding 41
switch
  electronic head switch 29
switch fabric connection 33

T

tape drive assembly 166
tape format specifications 5
tape head cleaner 41
tape length 18
tape media
  coating 20
  material 20
threading mechanism 29
Track Following 11
tracks
  number of 6
  positioning 7
TSM
  Managed System for SAN 75

U

Ultrium
  capacity 6
  cleaning cartridge 43
  media 87
  media features 225
  recording format 6
Ultrium 1
  capacity 18
  interfaces 35
  number of tracks 6
  performance 35
  tape length 18
Ultrium 2

capacity 18
channel calibration 38
interfaces 35
media features 225
multiple filemarks 38
number of tracks 6
performance 36
power management 38
speed matching 37
tape length 18
Ultrium Cartridge 18
Ultrium drive 28
display 39
Ultrium tape 9
universal cleaning cartridge 25
unload time 35–36

V

VHDCI 34
volume label format 23
volume serial number 22

W

wrap 14, 30
write process 14
write protect switch 24

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1556
Doc: 3690

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 3690
Doc:

IBM Redbooks

The IBM LTO Ultrium Tape Libraries Guide

(0.5" spine)
0.475"<->0.875"
250 <-> 459 pages

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1558
Doc: 3690

The IBM LTO Ultrium Tape Libraries Guide

Redbooks

Understand Linear Tape-Open technology and its unique architecture

Learn about the IBM Ultrium drives and libraries

Updated for Ultrium LTO 2 products

This IBM Redbook presents a general introduction to Linear Tape-Open (LTO) technology and the implementation of corresponding IBM products. As such it describes both general LTO technology specifications and specific details of the unique design of IBM Ultrium tape drives and libraries.

In addition to the description of LTO, the reader will find technical information about each of the IBM Ultrium products, including generalized sections about SCSI and Fibre Channel connections, multi-path architecture configurations, and tape technology comparisons with market positioning.

This book is intended for anyone who would like to understand more about the general LTO technology specification and how it came about, as well as the IBM implementation of that specification.

The second edition of this book covers the second generation LTO products as well as the original LTO products.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-5946-01 ISBN 0738453226

15426

Manual 7

2109 Model M12
User`s Guide

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1559
Doc: 3690

IBM TotalStorage SAN Switch

2109 Model M12 User's Guide

Read Before Using

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1560
Fls. Nº
3690
Doc:

GC26-7468-02

IBM TotalStorage SAN Switch

2109 Model M12 User's Guide

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1561
Doc: 3690

GC26-7468-02

Note:
Before using this information and the product it supports, read the general information in "Safety and environmental notices" on page xi and "Notices" on page 51.

Third Edition (May 2003)

This edition replaces GC26-7493-01.

© Copyright International Business Machines Corporation 2002, 2003. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables ix

Safety and environmental notices xi
Safety label checks xi
Environmental notices and statements xiii
Laser safety xiii
Battery notice xiv
Fire suppression systems xiv
Product recycling xiv
Product disposal xiv

About this document xv
Who should read this document xv
Additional information xv
2109 Model C36 with Model M12 library xv
Related documents xv
Web sites xvi
Getting help xvi
Getting software updates xvi
How to send your comments xvii

Introduction 1
Product overview 1
Throughput 2
Link distance 2
SFP fiber optic transceivers 2
System design overview 3
High availability 4
Reliability 4
Serviceability 5
Ports 5
Numbering 6
Rack mounting 6
Cooling system 6
Cable management 7
Worldwide name LED card 7
Power distribution system 7
Power distribution strategy 8
ac input 8
dc outputs 8
2N power architecture 8
CP blade assembly 9
CPU subsystem 9
Configuration 10
Management 10
Switch blade assembly 11
Switch blade assembly design 11
Fault monitoring and diagnostics 12
Diagnostic tests 12
System status indicators 12
Software features 13

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1562
Doc: 3690

Fabric OS 14
Interoperability 15
Security 15
Network manageability 15
Field replaceable units (FRUs) 16

Appendix A. Product specifications 17
2109 Model M12 components 17
Physical dimensions 17
2109 Model M12 and component weights 17
2109 Model C36 with Model M12 specifications 18
16-port card specifications. 18
CP card specifications 18
Facility specifications. 20
Power specifications 21
Environmental requirements 22
General specifications 22
Regulatory specifications 23

Appendix B. Safety certifications and regulatory compliance 25
Safety 25
EMI/EMC 25
Immunity 26

Appendix C. Danger and caution notice translations 27
Arabic 27
Brazilian-Portuguese 28
Chinese, simplified 29
Chinese, traditional 30
Croatian 31
Czech 32
Danish 33
Finnish 34
French 35
German 36
Greek 37
Hebrew. 38
Hungarian. 40
Italian 41
Japanese 42
Korean 43
Macedonian 44
Portuguese 45
Russian 46
Slovak 47
Slovenian 48
Spanish 49
Swedish 50

Notices 51
Trademarks 52
Electronic emission statements 52
Federal Communications Commission (FCC) statement 52
Industry Canada compliance statement 52
Chinese Class A compliance statement 52
European Community compliance statement 53

Germany compliance statement. 53
Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 54
Korean Government Ministry of Communication (MOC) statement 54
Taiwan class A compliance statement 54

Glossary 55

Index 69

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1563
Fls: Nº
3690
Doc:

Figures

1. Safety label on the 2109 Model M12 xii
2. Linecord caution label xii
3. SFP label (front view) xii
4. SFP label (back view) xiii
5. 2109 Model M12 (cable side and noncable side) 4

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1564
3690
Doc:

Tables

1. Brocade and IBM product and model number matrix. xvi
2. Power distribution system specifications 7
3. Power supply configurations 9
4. Cable side LEDs 12
5. Noncable side LEDs 13
6. Physical dimensions of the 2109 Model M12 17
7. Component weights 17
8. 2109 Model C36 with Model M12 specifications 18
9. Memory specifications 19
10. Battery specifications 19
11. Terminal serial port pinouts 19
12. Modem serial port pinouts 20
13. Power specifications 21
14. Environmental requirements 22
15. General specifications 22
16. Regulatory specifications 23

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1565
Doc: 3690

Safety and environmental notices

Safety notices are printed throughout this document.

A *danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

A *caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

An *attention* notice indicates the possibility of damage to a program, device, system, or data.

For translations of danger notices and caution notices, see Appendix C, "Danger and caution notice translations", on page 27. The notices are listed in numeric order based on their IDs, which are displayed in parentheses at the end of each notice. See the following examples of danger notices and caution notices for the location of the ID numbers.

DANGER

To prevent possible electrical shock during an electrical storm, do not connect or disconnect cables or station protectors for communications lines, display stations, printers, or telephones. (1)

CAUTION:
A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery may present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations. (1)

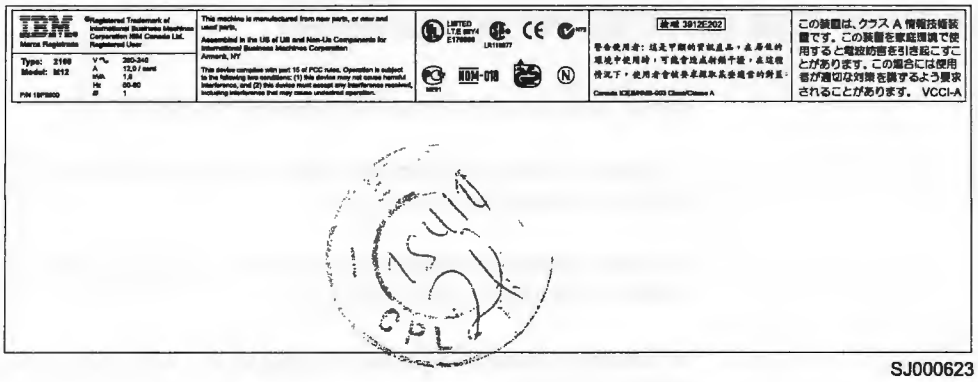
Safety label checks

Perform the following safety label checks:

1. Verify that the safety label shown in Figure 1 on page xii is installed on the 2109 Model M12.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
1566
Fls. Nº
Doc: 3690

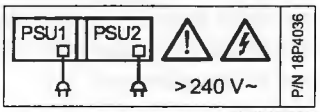


SJ000623

Figure 1. Safety label on the 2109 Model M12

2. Verify that the linecord safety label shown in Figure 2 is installed on the power supply of the 2109 Model M12.

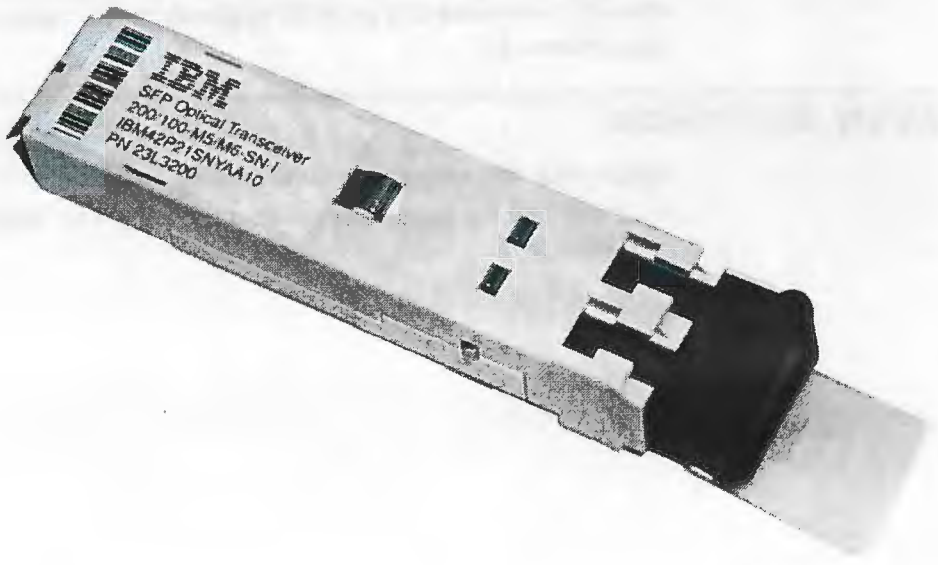
   CAUTION:
   This unit may have two linecords. To remove all power, disconnect both linecords. (1)



SJ000620

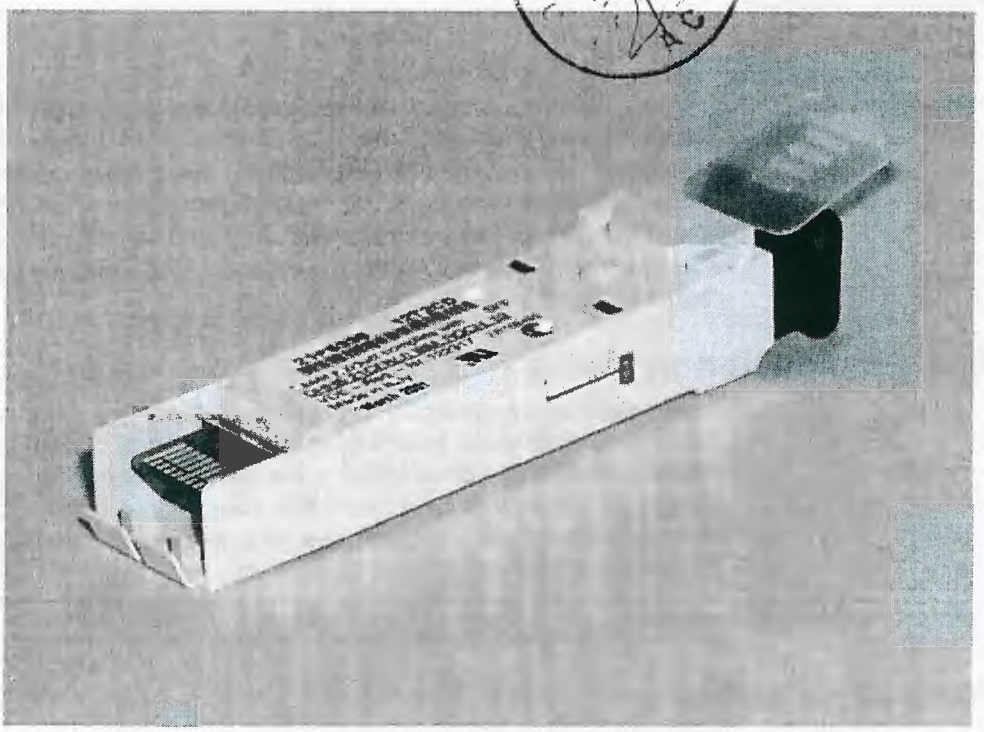
Figure 2. Linecord caution label

3. Verify that the SFP label shown in Figure 3 and Figure 4 on page xiii is installed on the 2109 Model M12.



SJ000317

Figure 3. SFP label (front view)



SJ000314

Figure 4. SFP label (back view)

Environmental notices and statements

This section describes the environmental notices and statements.

Laser safety

CAUTION:
In the United States use only GBIC units or Fibre-Optic products that comply with FDA radiation performance standards, 21 CFR Subchapter J. Internationally use only GBIC units or Fibre-Optic products that comply with IEC standard 825-1. Optical products that do not comply with these standards may produce light that is hazardous to the eyes.

SJ000327

This unit might contain a single-mode or a multimode transceiver Class 1 laser product. The transceiver complies with IEC 825-1 and FDA 21 CFR 1040.10 and 1040.11. The transceiver must be operated under the recommended operating conditions.

This equipment contains Class 1 laser products, and complies with FDA radiation Performance Standards, 21 CFR Subchapter J and the international laser safety standard IEC 825-2.

Usage restrictions

The optical ports of the modules must be terminated with an optical connector or with a dust plug.

CPMI – CORREIOS
1567
Fls. Nº
3690
Doc:

Battery notice

CAUTION:
A lithium battery can cause fire, explosion, or a severe burn. Do not recharge, disassemble, heat above 100°C (212°F), solder directly to the cell, incinerate, or expose cell contents to water. Keep away from children. Replace only with the part number specified for your system. Use of another battery may present a risk of fire or explosion. The battery connector is polarized; do not attempt to reverse the polarity. Dispose of the battery according to local regulations. (3)

Fire suppression systems

A fire suppression system is the responsibility of the customer. The customer's own insurance underwriter, local fire marshal, or a local building inspector, or both, should be consulted in selecting a fire suppression system that provides the correct level of coverage and protection. IBM designs and manufactures equipment to internal and external standards that require certain environments for reliable operation. Because IBM does not test any equipment for compatibility with fire suppression systems, IBM does not make compatibility claims of any kind nor does IBM provide recommendations on fire suppression systems.

Product recycling

This unit contains recyclable materials. These materials should be recycled where processing sites are available and according to local regulations. In some areas, IBM provides a product take-back program that ensures proper handling of the product. Contact your IBM representative for more information.

Product disposal

This unit might contain batteries. Remove and discard these batteries, or recycle them, according to local regulations.

About this document

This document introduces the IBM® TotalStorage™ SAN Switch 2109 Model M12 (hereafter referred to as the 2109 Model M12).

Who should read this document

This document is intended for network and system administrators whose responsibilities include administering and managing a storage area network (SAN).

Additional information

This section contains the following information:

- A list of the documents in the 2109 Model C36 with Model M12 library
- A list of the related documents
- The available Web sites
- Instructions on how to get help
- Instructions on how to get software updates
- Information about how to send your comments

2109 Model C36 with Model M12 library

The following documents contain information related to this product:

- *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*, GC26-7467
- *IBM TotalStorage SAN Switch 2109 Model M12 User's Guide*, GC26-7468 (this book)

Related documents

Information related to the 2109 Model M12 software can be found in the following documents:

- *Brocade Advanced Performance Monitoring User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Diagnostic and System Error Message Reference*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Reference*
- *Brocade Fabric Watch User's Guide*
- *Brocade ISL Trunking User's Guide*
- *Brocade MIB Reference*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Silkworm 12000 Core Migration User's Guide*
- *Building and Scaling Brocade SAN Fabrics: Design and Best Practices Guide*

When you use any of the Brocade documents, you will notice that the model numbers reflect the original Brocade switches. Table 1 on page xvi provides a product matrix for you to use to correlate the Brocade model numbers to the IBM

© Copyright IBM Corp. 2002, 2003

Fls. Nº 1568
Doc: 3690

product and model numbers.

Table 1. Brocade and IBM product and model number matrix

Brocade model number	IBM product and model number
Silkworm 2010	3534 Model 1RU
Silkworm 2400	2109 Model S08
Silkworm 2800	2109 Model S16
Silkworm 3200	3534 Model F08
Silkworm 3800	2109 Model F16
Silkworm 3900	2109 Model F32
Silkworm 12000	2109 Model M12

Web sites

For detailed information about models and firmware that the switch supports, see the following Web site:

www.ibm.com/storage/fcswitch/

For detailed information about Fibre Channel standards, see the Fibre Channel Association Web site at:

www.fibrechannel.com/

For a directory of worldwide contact information, including technical support, see the following Web site:

www.ibm.com/contact/

Getting help

Contact your switch supplier for technical support. This includes support of hardware, all product repairs, and ordering of spare components.

Be prepared to provide the following information to the support personnel:

- The switch serial number
- The switch worldwide name
- The topology configuration
- Any output from the **supportShow** Telnet command
- A detailed description of the problem
- Any troubleshooting steps that were already performed

Getting software updates

Contact your software vendor for software updates and maintenance releases.

For utility programs to facilitate loading firmware, sample Fabric Watch configurations, and management information base (MIB) files for switch management by simple network management protocol (SNMP), see the following Web site:

www.storage.ibm.com/ibmsan/products/sanfabric.htm

How to send your comments

Your feedback is important to help us provide the highest quality of information. If you have any comments about this document, you can submit them in one of the following ways:

- E-mail

  Submit your comments electronically to:

  starpubs@us.ibm.com

  Be sure to include the name and order number of the document and, if applicable, the specific location of the text that you are commenting on, such as a page number or table number.

- Mail or fax

  Fill out the Readers' Comments form (RCF) at the back of this document and return it by mail or fax (1-800-426-6209) or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

  International Business Machines Corporation
  RCF Processing Department
  Dept. M86/Bldg. 050-3
  5600 Cottle Road
  San Jose, CA 95193-0001
  U.S.A.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1569
3690
Doc:

Introduction

This chapter describes the TotalStorage SAN Switch 2109 Model M12, hereafter referred to as the 2109 Model M12. It provides the following information:

- "Product overview"
- "System design overview" on page 3
- "Power distribution system" on page 7
- "CP blade assembly" on page 9
- "Switch blade assembly" on page 11
- "Fault monitoring and diagnostics" on page 12
- "Software features" on page 13
- "Field replaceable units (FRUs)" on page 16

Product overview

The 2109 Model M12 represents the next generation of advanced Fibre Channel switches that are used to intelligently interconnect storage devices, hosts, and servers in a storage area network (SAN). It is a revolutionary product, a dual 64-port Fibre Channel switch that delivers unprecedented performance, scalability, flexibility, functionality, reliability, and availability.

- The 2109 Model M12 delivers a very high-density port, rack-ready solution to drive cost-effective SAN.
- The dual switch capability allows either one or two 64-port switches per chassis. You can interconnect the switches to create a high port count solution, or you can use them in a dual fabric, high availability topology.
- The 2109 Model M12 supports 1 Gbps and 2 Gbps auto-sensing Fibre Channel ports. Trunking technology groups up to four ports together to create high performance 8 Gbps inter-switch links (ISL) trunks between switches.
- Universal ports self-configure as expansion ports (E_ports), fabric ports (F_ports), or fabric loop ports (FL_ports).
- Small form-factor pluggable (SFP) optical transceivers support any combination of short wavelength (SWL) and long wavelength (LWL) optical media on a single switch module.
- The 2109 Model M12 offers a high availability platform for mission-critical SAN-designed applications.
- Dual redundant control processors (CPs) provide high availability and enable nondisruptive software upgrades.
- The 2109 Model M12 offers forward and backward compatibility with all 3534 and 2109 series switches.
- The Fabric operating system (OS) delivers distributed intelligence throughout the network and enables a wide range of value-added applications including Extended Fabrics, Fabric Access, Fabric Watch, Remote Switch, Web Tools, Secure Fabric OS, Advanced Zoning, and Advanced Security feature.
- High availability redundant design, extensive diagnostics, and system monitoring capabilities integrated with Fabric OS management tools deliver unprecedented reliability, availability, and serviceability.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1570
3690
Doc:

The 2109 Model M12 is a nonblocking core fabric switch. It never prevents a server from being able to connect to storage, even under congestion. The backplane bandwidth between ports on a 2109 Model M12 is sufficient to allow traffic to flow at full bandwidth.

Throughput

The 2109 Model M12 provides continuous and sustained bandwidth to all ports in a single or dual 32-port or 64-port switch scenario at their rated line speed. Throughput is 2.125 Gbps inbound and outbound per port. All ports can be simultaneously loaded for up to 100% utilization at full bandwidth. The backplane can handle future support for a 128-port switch, 10 bps Fibre Channel, IP connectivity, application processing and Infiniband.

Each port on the 2109 Model M12 is auto-sensing and supports 1 Gbps or 2 Gbps speeds. You can manually set the ports to support either 1 Gbps or 2 Gbps links. The ports perform speed-matching, which allows 1 Gbps and 2 Gbps links to mix on any route within the fabric. When there is 1 Gbps in and 2 Gbps out, the ASIC delays transmitting the outbound frame until half the frame is received at 1 Gbps. With 2 Gbps in and 1 Gbps out, the ASIC delays releasing the buffer to ensure that the 1 Gbps transmit port has adequate time to empty it.

Link distance

The 2109 Model M12 operates at up to 10 km (6.21 mi) at both 1 Gbps and 2 Gbps speed settings and supports LWL SFPs and single-mode fiber.

By using the Extended Fabrics optional software feature, the switch operates at distances greater than 10 km (6.21 mi) by using various methods. The switch leverages the current dense wavelength division multiplexing (DWDM) certification and is certified to interoperate with equipment from Optical Networks, Cisco Systems, Inc., Nortel Networks, and other leading vendors.

The switch operates at near full link speed at distances up to 100 km (62.13 mi) for 1 Gbps or 50 km (31.06 mi) for 2 Gbps speeds using the Extended Fabrics feature.

For information about Extended Fabrics, see the *Brocade Distributed Fabric User's Guide.*

SFP fiber optic transceivers

Each blade assembly supports up to 16 SFP fiber optic transceivers that convert electrical signals to optical signals (and optical signals to electrical signals) and are capable of transmitting at both 1 Gbps and 2 Gbps speeds.

Each SFP fiber optic transceiver supports 850 nm SWL, on multimode fiber optic cable, or 1310 nm LWL, on single mode fiber optic cable. These miniature optical transceivers meet the high port density that is available in the 2109 Model M12, deliver twice the port density of standard removable gigabit interface converter (GBIC) transceivers, and are encased in metal or shielded plastic to ensure low emissions and high thermal management. SFP devices are hot-swappable and connections are through industry-standard LC connectors.

System design overview

The 2109 Model M12 is highly available, modular, and scalable. High availability features include:

- Redundant CPs and CP hot-swappable replacements
- Dual redundant ac input and hot-swappable power supplies in the redundant power subsystem
- Hot-swappable blowers in the redundant cooling system
- Hot-swappable switch modules

The modular multi-blade assembly chassis of the 2109 Model M12 consists of:

- Up to eight hot-swappable 16-port switch blade assemblies that deliver up to two separate 64-port Fibre Channel switches in a single chassis. Each 64-port switch uses four blade assemblies.
- Two slots for CP blade assemblies

  A single active CP can control both logical switches in the chassis.
- Modular hot-swappable field replaceable units (FRUs):
  - Switch blade assembly
  - CP blade assembly
  - SFP optical transceivers
  - Blower assembly
  - Power supply
- Cables, blade assemblies, and power supplies that are serviced from the cable side of the switch, and blowers that are serviced from the noncable side. See Figure 5 on page 4, which illustrates the cable side and noncable side of the switch.
- A cable management tray and cable pillars
- Three blowers that provide cooling for the switch. The switch continues to operate indefinitely even if one blower fails.
- A worldwide name (WWN) light-emitting diode (LED) card on the noncable side that maintains chassis-specific information, such as WWNs, Internet Protocol (IP) addresses and summary status information of each blade assembly and power supply

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1571
Doc: 3690

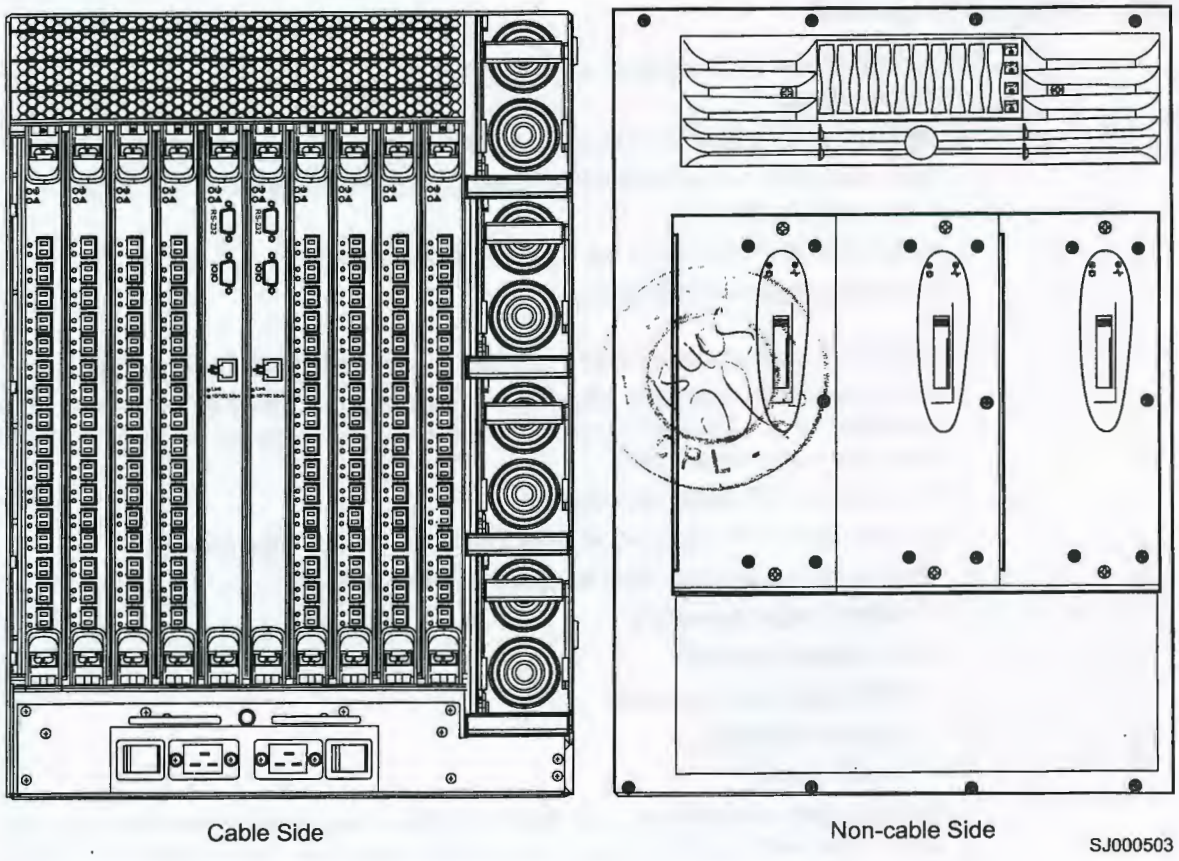


Figure 5. 2109 Model M12 (cable side and noncable side)

High availability

If a system is available, it is accessible 7 days a week and 24 hours per day. Availability is designated in terms of 9s. For example, the architecture of the 2109 Model M12 is designed for availability in excess of 99.999%.

The high availability software architecture of the 2109 Model M12 provides a common framework for all applications that reside on the system. High availability allows global and local states to be maintained so that any component failure is fully manageable.

Reliability

In addition to being available, the system must be reliable. This means that some, if not all, of its state must be maintained. In a reliable system, you are not aware of the internal state of a switch, and you experience continued system service with zero degradation.

The 2109 Model M12 provides the following features to ensure reliability:

- An error detection and correction mechanism to protect all data in the switch
- Power-on self test (POST)
- Error detection and fault isolation, such as cyclic redundancy checking (CRC), parity checking, checksum, and illegal address checking

- Dual CPs that enable hot, nondisruptive fast firmware upgrades. Each CP contains two serial ports and one Ethernet port. Offline CP diagnostics and remote diagnostics make troubleshooting easy. The Standby CP continuously runs diagnostics to ensure that it is operational should a failover be necessary.
- Inter-IC (I^2C) monitoring and control

For information about diagnostics, see the *Brocade Diagnostic and System Error Message Reference.*

Serviceability

The 2109 Model M12 provides the following features to enhance and ensure serviceability:

- Modular design with hot-swappable components
- Redundant flash memory that stores two firmware images per CP
- Extensive diagnostics and status reporting, along with a serial port to support an external, country-specific modem for remote diagnostics and status monitoring
- Nonvolatile random-access memory (NVRAM) that contains the OEM serial number, IBM serial number, revision information, and part number information
- Background health check daemon
- Memory scrubber, self test, and bus ping to determine if a bus is not functioning
- Watchdog timers
- Status LEDs
- Predictive diagnostics analysis through Fabric Watch
- SNMP integration with higher layer managers

For information about diagnostics, see the *Brocade Diagnostic and System Error Message Reference.* For information about Fabric Watch, see the *Brocade Fabric Watch User's Guide.*

Ports

Each switch blade assembly houses 16 auto-sensing 1 Gbps or 2 Gbps Fibre Channel ports and uses SFP optical transceivers.

The 2109 Model M12 supports the following port types:

- Optical ports
- Ethernet port
- Serial port

Optical ports

Fibre Channel interfaces of the 2109 Model M12 are equipped with an optical port interface that uses an SWL, 780 to 850 nm, or an LWL, 1270 to 1350 nm, laser transmitter. The laser complies with FDA21 CFR (J) Class 1 laser safety requirements. It uses non-Open Fibre Control (OFC) optical SFPs in the 2109 Model M12 series circuit. Safe Class 1 operation is guaranteed by limiting the optical power that is emitted by the port, which eliminates the need for physical shutters.

The optical SFP uses the LC-duplex connector scheme.

Ethernet ports

The 2109 Model M12 provides a fully IEEE compliant 10BASE-T or 100BASE-T Ethernet port for switch management. The port has two LEDs that indicates

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1572
Doc: 3690

- Speed (10 Mbps or 100 Mbps)
- Status of the connection

Additionally, each CP has its own Ethernet port. You can choose to connect the Ethernet ports to each other through an Ethernet switch or to connect them to separate networks for greater availability. Each CP has its own unique IP address and is accessible independent of the other CP.

Serial ports

Each CP comes with two serial ports. The top serial port on the installed CP is an RS-232 port that is used for remote dial-in. The bottom port is used for accessing the console.

Numbering

The 2109 Model M12 employs a numbering scheme that progresses from left to right and bottom to top in numerical order. The reference location is from the cable side of the chassis.

- Blade assemblies are numbered from 1 - 10, from left to right.
- Ports are numbered from 0 - 15, from bottom to top.
- Power supplies are numbered from 1 - 4, from bottom to top.
- Blowers are numbered from 1 - 3, from left to right.

Rack mounting

The mechanical design of the 2109 Model M12 allows rack mounting with either the cable side or the noncable side facing the front of the equipment rack. The chassis fits into a standard 19-inch EIA rack. Each chassis measures:

- 43.74 cm (17.22 in.) wide
- 70.87 cm (27.9 in.) deep (without the door)
- 61.24 cm (24.11 in.) high (less than 14U)

Cooling system

The 2109 Model M12 uses a redundant system of three hot-swappable blowers. Cool air intake is from the noncable side of the chassis, is pressurized, and is forced through the system. Heated air exits at the top of the cable side of the chassis. Three blowers that are used in conjunction with a pressurized plenum cool the unit. Each blower assembly includes a blower control assembly, which provides the following features:

- Blower status LEDs
- Blower speed sensing
- Blower speed control
- Serial electronically erasable programmable read only memory (EEPROM) that contains the part number, revision level, and error logs for the blade assembly
- Inlet air temperature monitoring

The 2109 Model M12 operates indefinitely if a single blower fails. When a blower assembly is removed, a mechanical flap seals the air chamber to maintain positive cooling air pressure in the chassis while the failed blower assembly is being replaced.

Cable management

The cable management tray and cable pillars provide easy access to the 2109 Model M12 cables and allow you to organize and maintain the cables easily. Up to 128 pairs of fibre optic cables can be maintained on a single chassis. The cable management system is designed to allow any switch module to be replaced without disrupting service on any adjacent blade assemblies.

Worldwide name LED card

The WWN LED card is the neutral location to accommodate the worldwide unique serial ID for each logical switch on the 2109 Model M12. It is an integral part of the chassis. The serial EEPROM device contains multiple serial numbers for identifying the chassis, back plane, and the WWN card itself.

As an alternative system status indicator, this card consolidates the status of all modular components in the system on the cable side and presents the status to you in the form of LEDs on the noncable side. The arrangement of the LEDs on this card resembles the look of status LEDs on the other side of the switch.

The LEDs provide the summary of cable-side system status on the switch as follows:

- Two LEDs per blade assembly on the cable side of the cabinet
  - Green indicates that the power is OK.
  - Amber indicates that the blade needs attention.
- Two LEDs per power supply. Both LEDs are in the same location.
  - Green indicates that the power is OK.
  - Amber indicates that the power supply needs attention.

Power distribution system

The power subsystem is a redundant +48 V dc power distribution system with a provision for up to four 1000-watt, 48 V dc bulk power supplies. Bulk power supplies produce the intermediate distribution voltage in the distributed power system. See Table 2 for the power distribution system specifications.

Table 2. Power distribution system specifications

Specification	Value
Input voltage	A fully loaded switch requires a maximum of 2200 Volt-Amps. This results in a mains current of 9 amps at 240 V ac line voltage or 10 amps at 208 V ac line voltage. The rated ac input range is 180 - 264 V ac.
Supported power range	Nominal: 200 - 240 V ac, single phase
Input frequency range	47 - 63 Hz
Power supplies (each)	Output voltages: 48 V at 20 amps; 12 V at 4 amps Maximum output power: 1000 watts
ac inrush current	40 amps maximum, peak
Ride through	The power supply outputs remain within specified regulation for a minimum of 20 msec after the ac mains are disconnected.

RCS nº 02/2005 - CN
CPMI - CORREIOS
Fls. Nº 1573
Doc: 3690

Table 2. Power distribution system specifications (continued)

Specification	Value
Under voltage protection	The 2109 Model M12 power supply self-protects from any input voltage, static or dynamic, from zero volts to its operating ranges. It recovers to normal operation when it returns to its operating range.

Power distribution strategy

All power for the blades comes from a single 48 V intermediate power bus. Great care is taken at each load to assure the integrity of the power bus.

The power supplies also provide a separate 12 V AUX voltage. This is used throughout the system to power the I²C logic and to monitor and control different system states.

ac input

Each ac input has an on-off circuit breaker switch. The power supply modules include input power filtering and power indicator LEDs. The power supply output remains within specific regulation for a minimum of 20 msec after the ac mains have been disconnected.

Two detachable line cords provide ac input power to the chassis.

dc outputs

The 2109 Model M12 uses up to four power supplies. All power supplies are hot-swappable. Two power supplies receive input power from one of the ac inputs. The remaining two power supplies receive power from the other ac input. Only two power supplies are required to run a completely loaded chassis. Therefore, if one ac input fails, and all power supply modules are populated, the chassis continues to run uninterrupted. If a power supply module fails, the remaining power supply modules continue to provide uninterrupted power to the chassis. The power supplies are plugged directly into their power bays to an internal blind connector.

Each blade assembly has separate dc-dc converter bricks for each voltage that is required. This allows local regulation at the blade assembly, and provides for future flexibility to match voltage needs with blade assembly type.

To maximize system availability when the switch blade assembly is plugged, it is initially powered off by the hardware. This ensures that adding a blade assembly does not bring the whole switch down if inadequate power is available. The system confirms sufficient power for the new module and then applies power. If sufficient power is not available (for example, if only one of the possible four power supplies are installed), the system does not allow more than four switch blade assemblies plus two CP blades to be powered up.

2N power architecture

The 2N power architecture is designed to protect against the loss of ac power. The 2109 Model M12 offers four power supply modules to assure maximum availability. Under normal operating conditions, only two power supplies are needed for full system operation. However, to ensure redundancy, two additional power supplies are available and are added in pairs, one per ac source.

Table 3 shows various supported power supply configurations and their respective levels of redundancy.

Table 3. Power supply configurations

Number of power supplies	Number of power cords	Number of switch blades	Number of CP blades	Number of blowers	Redundancy
1	1	4	2	3	No
2	1	4 or 8	2	3	Partial (See note)
3	2	4	2	3	Yes
4	2	8	2	3	Yes
Note: A single power cord results in the lack of ac source redundancy.					

CP blade assembly

The CP blade assembly controls the following 2109 Model M12 functions or features:

- System initialization
- Switch drivers
- High availability drivers
- Name server
- System management
- Fabric OS
- Fabric Manager
- Extended Fabrics
- Fabric Watch
- Remote Switch
- Web Tools
- Zoning

The CP blade assembly is compliant with the PCI Local Bus Specification 2.1. It provides all control and management functions in a 2109 Model M12 platform.

For more information about these features, see the following documents:

- *Brocade Fabric Watch User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Reference*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Advanced Zoning User's Guide*

CPU subsystem

The PowerPC 405GP 200-MHz microprocessor (PPC405) resides on the CP blade assembly. It contains a high-performance reduced instruction-set computer (RISC) core, synchronous dynamic random access memory (SDRAM) controller, PCI bus

CPMI - CORREIOS
Fls. Nº 1374
Doc: 3690

interface, direct memory access (DMA) engine, serial ports, I²C interface, read-only memory, and general purpose I/O. In addition, the CP blade assembly has the following functions:

- SDRAM controller that is built into the PPC405 with error correction support at 100 MHz
- SDRAM that supports 128 Mb configuration
- Socket PLCC32 boot flash that supports 512 Kb
- On-board compact flash that supports 256 Mb of software storage
- Two 32-bit, 33 MHz PCI-PCI bridges nontransparent
- Hot-plugged interface circuitry to support reliability, availability, serviceability and failover. If one device stops functioning, the other device automatically takes its place.
- One 10 Mbps or 100 Mbps management connection (RJ-45 connector type)
- Two universal asynchronous receiver-transmitter (UART) serial ports: one modem port for remote diagnostic testing and one terminal port for Telnet and command line interface (CLI) communication
- One amber LED to indicate the status for CP errors
- One green LED to indicate the proper operation for the CP power
- One green LED to indicate the system Ethernet 10 Mbps or 100 Mbps speed
- One amber LED to indicate the system Ethernet link status
- One digital thermometer for temperature sensing
- One real-time clock (RTC) with battery
- Two I²C I/O expander devices

Configuration

The CP blade assemblies can be configured to support a single 2-blade assembly topology, dual 2-blade assembly topology, a 4-blade assembly topology, a dual 4-blade assembly topology, or an 8-blade assembly switch topology. Other topologies can be supported on an as needed basis. Each CP interfaces to switch blade assemblies using a standard Peripheral Component Interconnect (PCI) bus. This bus runs at 33 MHz and can be 32 or 64 bits wide (bus 1 and 2). The CP blade assembly supports the following switch configurations:

- Single 32-port switch with dual CPs
- Dual 32-port switches with dual CPs
- Single 64-port switch with dual CPs
- Dual 64-port switches with dual CPs

Management

The CPs manage as many as eight switch blade assemblies within a single switch and monitor up to four power supplies, three blowers, three inlets (in the blower), up to 12 outlet temperature monitors (one per blade assembly), and other blade assembly-specific environmental features, such as voltages. The CP can individually reset each blade assembly, detect the status of each blade assembly (installed/not installed), manage the interrupt and service demand from each blade assembly, control the ability of a blade assembly to drive or not drive the PCI bus, and determine the error status of each blade assembly.

Switch blade assembly

The switch blade assembly is a blade in the chassis of the 2109 Model M12. Each switch blade assembly provides 16 external Fibre Channel ports that run at 1 Gbps and 2 Gbps. A full switch consists of up to four switch blade assemblies and provides up to 64 ports in multiples of 16 ports.

The switch blade assembly is responsible for Fibre Channel switch circuitry and houses the switch application-specific integrated circuit (ASIC), backplane serial-deserializer (SERDES), external SERDES, and status LEDs for external SERDES such as port speed and port state, as well as the SFP fiber optic media. The SERDES performs two key functions. It receives the serial data stream of the system and converts it to a parallel stream. It also transmits parallel data streams to serial data streams.

Each switch blade assembly is hot-swappable and can be installed while the switch is running. Long pins, short pins, or both are used on the backplane to assure proper ground-voltage-signal sequencing. Field effect transistor (FET) switches, such as QuickSwitches, are used to isolate the PCI interfaces.

When a switch blade assembly is inserted, the power regulation circuitry inhibits the on-board dc converter (DCC) and maintains the switch blade assembly as turned off. The CP, under software control, enables the DCC and thus turns on the switch blade assembly. When the switch blade assembly is ready it interrupts the CP for initialization.

Each switch blade assembly has an on-board serial EEPROM that is only accessible through the I²C bus interface. This serial EEPROM can be accessed by a CP to determine information, including:

- OEM serial number
- IBM serial number
- Manufacturing date
- Manufacturing location
- Part number
- Revision
- Error logs

Switch blade assembly design

The switch blade assembly has the following dimensions:

- 42.06 cm (16.56 in.) high
- 29.74 cm (11.71 in.) wide
- 3.58 cm (1.41 in.) deep

Each switch blade assembly is connected to the backplane through high performance connectors.

The switch blade assembly provides 16 external Fibre Channel ports. Each of the 16 ports per blade assembly are auto-sensing, speed matching at 1 Gbps and 2 Gbps, support trunking, and are universal (E_port, F_port, and FL_port). Port speed can be managed through the management interface.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1575
3690
Doc:

Fault monitoring and diagnostics

Fault monitoring, diagnostic tests, and system status indicators simplify switch management and ensure the availability of the 2109 Model M12.

Diagnostic tests

Diagnostic testing occurs in three areas: power-on self test (POST), switch level testing, and manufacturing tests.

- The POST tests are blade oriented and ensure that the switch is ready for use. Testing is performed on physical ports.
- Switch level tests are done at the user port level. The tests rely on the standard Fabric OS support to provide routing and port setup.
- Manufacturing support includes long duration testing.

System status indicators

LEDs on the noncable side of the switch summarize the system status of each switch blade assembly, each CP blade assembly, and each power supply module. The blowers, which are accessible on the noncable side, also have LEDs that indicate their status.

Cable-side LEDs

Table 4 describes the appearance of the LEDs on the cable side of the system:

Table 4. Cable side LEDs

LED location	Indication
System status panel	• Green indicates that the blade assembly has power. • Amber indicates that the blade assembly needs attention.
CP blade assembly	Contains two additional LEDs for its Ethernet ports • Green indicates link speed. – On indicates 100 Mbps operation. – Off indicates 10 Mbps operation. • Amber indicates link status – Solid on indicates a link is not good. – Flashing indicates a link is OK. – Off indicates that no link is detected.
Each port on a switch card	Contains two LEDs • Top LED: – Green indicates 2.125 Gbps. – Off indicates 1.0625 Gbps. • Bottom LED: – Green indicates the port is operational. – Amber indicates the port is off or disabled.

Table 4. Cable side LEDs (continued)

LED location	Indication
Each power supply	Contains three LEDs • Green – Solid indicates that ac is applied and power outputs are OK. – Flashing indicates that only the auxiliary output is valid. • Amber center light is a predictive failure light. It indicates that a power supply might fail due to a poorly performing fan. A replacement should be scheduled soon. • Amber lower light is a fault light. It indicates that a power supply has failed and a replacement is necessary.

Noncable side LEDs

Table 5 describes the appearance of the LEDs on the noncable side of the system:

Table 5. Noncable side LEDs

LED location	Indication
Blower	• Green indicates that the blade assembly has power. • Amber indicates that the blade assembly needs attention.
Blower system status panel	• Green indicates that the blower assembly has power. • Amber indicates that the blower assembly needs attention.

Additional status reporting functions are provided by the Fabric Watch feature. For information about Fabric Watch, see the *Brocade Fabric Watch User's Guide*.

Software features

Fabric OS version 4.1 supports the 2109 Model M12. Fabric OS includes all the basic switch and fabric support software as well as optionally licensed software that is enabled by using license keys. Fabric OS is made up of two major software components: firmware that initializes and manages the switch hardware, and diagnostics.

Optionally licensed and separately priced features include:

- Extended Fabrics (Feature code 7603)

  Provides up to 100 km (62.14 mi.) of switched fabric connectivity at full bandwidth over long distances
- Remote Switch (Feature code 7602)

  Enables switches to interconnect over wide area network (WAN) using third-party gateway solutions that support FC over IP, FC over ATM, and FC over SONET
- Advanced Security (Feature code 7623)

CPMI - CORREIOS
Fls. Nº 1576
Doc: 3690

Enables policy-based security mechanisms that are integrated within Fabric OS

The following licensed software provides a graphical user interface from a standard workstation:

- Fabric Manager 4.0 (Feature code 7203)

  Administers, configures, and maintains fabric switches and SANs with host-based software

The following licensed features are included with the 2109 Model M12:

- Performance Monitoring

  Comprehensive tool for monitoring the performance of network storage resources
- ISL Trunking

  Connects up to four ISLs between two switches through an expansion port (E_port) to merge logically into one link
- Fabric Watch

  Monitors mission-critical fabric parameters
- Advanced Zoning

  Segments a fabric into virtual private SANs
- Web Tools

  Administers, configures, and maintains fabric switches and SANs

Note: To activate these features, go to the following Web site:

www.ibm.com/storage/key/

See the following documents for more information about Fabric Watch, Fabric Manager, Web Tools, Secure Fabric OS, and high availability:

- *Brocade Fabric Watch User's Guide*
- *Brocade Fabric Manager User's Guide*
- *Brocade Advanced Web Tools User's Guide*
- *Brocade Distributed Fabric User's Guide*
- *Brocade Advanced Zoning User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Fabric OS Reference*
- *Brocade Silkworm 12000 Hardware Reference Manual*

Fabric OS

Fabric OS is a robust operating system for high-performance, scalable SANs. Fabric OS allows you to:

- Rapidly build highly resilient, fault-tolerant multiswitch SAN fabrics
- Ensure high-speed access to business-critical data
- Allow hosts to dynamically share storage resources
- Rapidly scale the SAN by simply plugging in new devices with no configuration required. Software upgrades are nondisruptive
- Integrate private loops, private hosts, load balancing and sophisticated SAN management
- Easily manage the switches, hosts and devices that comprise the SAN

The Fabric OS for the 2109 Model M12 allows any Fibre Channel-compliant device to attach to the switches as long as it conforms to the device login, name service, and related Fibre Channel feature standards. Each operating environment requires that a Fibre Channel host bus adapter (HBA) be available with a standards-compliant driver for proper interface to the fabric.

Fabric OS consists of a set of embedded applications that run on top of an embedded real-time Linux operating system kernel. These applications include the following:

- Name server
- Alias server
- Simple Network Management Protocol (SNMP) agent
- Several tasks to manage the following:
  - Address assignment
  - Routing
  - Link initialization
  - Fabric initialization
  - Link shutdown
  - Switch shutdown
  - User interface

Interoperability

Fabric OS Version 4.1 interoperates with 3534 Model 1RU (minimum version 2.6). McData ED-5000 (from operating system version 4.0) interoperability is also provided.

Security

Secure Telnet access is available using Secure Shell (SSH), a network security protocol for secure remote login and other secure network services over an insecure network.

Web Tools management is available through a secure browser by using Secure Sockets Layer (SSL). The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Because SSL is built into all major browsers and Web servers, installing a digital certificate turns on the SSL capabilities. For more information about Web Tools, see the *Brocade Advanced Web Tools User's Guide*.

Network manageability

The entire switch is managed as a single element and appears as a single element to a Network Management System (NMS). Each 64-port switch responds to its own IP address and appears as a separate entity to the Telnet protocol and the SNMP.

The management interfaces include blade assemblies as an intermediate component between switches and ports. In addition, all management interfaces such as, Telnet, Web Tools, the Fabric Access Layer API, and Management Server, support a "port N within blade M" naming scheme.

When SNMP devices send SNMP messages to a management console running SAN management software, the information is stored in a Management Information Base (MIB). The Fabric OS Version of the 2109 Model M12 supports the latest

CPMI - CORREIOS
Fls. Nº 1577
Doc: 3690

Fibre Alliance Fibre Channel management (FCMGMT) MIBs, which allow common information necessary for management software to provide information to a SAN administrator.

Field replaceable units (FRUs)

Each FRU in the 2109 Model M12 is hot-swappable. Fault isolation to the FRU level provides failure containment. Each FRU can be identified remotely with the FRU part number, serial number, and revision level.

The FRUs of the the 2109 Model M12 include:

- Chassis, including backplane, blower and power supply backplane, ac harness, and blower harness (does not include blower assemblies or power supplies)
- 16-port Fibre Channel switch module
- CP
- Power supply (180 - 264 V ac, 1000 W)
- Blower assembly, including blower, control board, and housing
- Rear LED status panel cosmetic trim panel
- Chassis door
- Card slot filler panel
- Power supply filler panel
- Cable management tray
- Optical cable management guides (package of 16)
- Rack mount kit, including rear brackets and bottom support rack rails
- Optional mid-mount rack kit
- ac input cable: North America, UK, continental Europe, Australia and New Zealand, and international IEC 60309
- Serial cable
- SFP SWL transceiver
- SFP LWL transceiver

For more information about the FRUs, see the *IBM TotalStorage SAN Cabinet 2109 Model C36 with Model M12 Installation and Service Guide*.

The CP dynamically isolates any FRU that is nonfunctional for ease of repair and replacement as well as to prevent a nonfunctional blade assembly from affecting system availability. Each switch blade assembly has 128K bits of nonvolatile memory and takes inventory of the system and determines the contents of the system electronically. For example, you can perform the following tasks:

- Determine how long components have been running when they fail
- View error logs
- View operating hours
- View log histories to determine MTBF

For more information about how to perform these tasks, see the *Brocade Fabric OS Reference*.

Appendix A. Product specifications

This appendix contains the 2109 Model C36 with Model M12 specifications.

2109 Model M12 components

The 2109 Model M12 contains the following components:

- A 14U chassis, designed to be mounted in a 48.26 cm (19 in.) rack. Two 2109 Model M12 switches can be mounted in a 2109 Model C36 cabinet.
- 16-port cards in configurations up to eight cards per chassis, with 16 optical ports per card, compatible with SFPs.
- Two CP cards, each with:
  - One modem serial port with a DB-9 connector (full RS-232)
  - One terminal serial port with a DB-9 connector (RS-232 signal subset)
  - One IEEE compliant RJ-45 connector for use with a 10 Mbps or 100 Mbps Ethernet connection
  - A real-time clock (RTC) with a 10-year battery and 56 bytes of NVRAM
- Four power supplies with built-in fans. The power supplies plug into internal blind-mate connectors when installed in the chassis.
- Two ac power inlet connectors with ac power switches (power panel).
- A WWN card and bezel.
- Three blower assemblies for forced-air cooling of the 16-port cards and the CP cards.

Air enters inlet vents on the blower assembly side of the chassis and exits through vents on the port side of the chassis. The blower speed is governed by inlet air temperature. The blowers go into high speed when the inlet air temperature exceeds 33°C (91°F).

Physical dimensions

The dimensions of the 2109 Model M12 are listed in Table 6.

Table 6. Physical dimensions of the 2109 Model M12

Dimension	Value
Height	14U (24.11 in.)
Depth	70.9 cm (27.9 in.)
Depth with door	72.9 cm (28.7 in.)
Width	43.7 cm (17.2 in.)

2109 Model M12 and component weights

The weight of a fully-loaded 2109 Model M12, as well as the weights of individual components, are listed in Table 7.

Table 7. Component weights

Component	Weight
Fully loaded chassis	Approximately 114 kg (250.0 lbs)
Empty chassis	47.1 kg (104.0 lbs)

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1578
Doc: 3690

Table 7. Component weights (continued)

Component	Weight
Door	3.4 kg (7.6 lbs)
Blower assembly	4 kg (8.8 lbs)
Power supply	3.2 kg (7.0 lbs)
WWN bezel	0.27 kg (0.6 lbs)
CP card	2.5 kg (5.6 lbs)
16-port card	3.9 kg (8.6 lbs)
Card filler panel	1.6 kg (3.2 lbs)
Cable management tray	0.27 kg (0.6 lbs)

2109 Model C36 with Model M12 specifications

The specifications for the 2109 Model C36 with Model M12 are listed in Table 8.

Table 8. 2109 Model C36 with Model M12 specifications

Dimension	Value
Height	1785 mm (70.3 in.)
Depth	• With rear door installed: 1042 mm (41 in.) • With rear and front door installed: 1098 mm (43.3 in.)
Width	• With side panels installed: 650 mm (25.6 in.) • Without side panel installed: 623 mm (24.5 in.)
EIA units	36 EIA units
Weight	Cabinet with two 2109 Model M12 switches: 816 kg (1795 lbs)

16-port card specifications

The ports in the 2109 Model C36 with Model M12 support full-duplex link-speeds at 2.125 Gbps or 1.0625 Gbps, inbound and outbound, automatically negotiating to the highest common speed of all the devices that are connected to the port. Each port has a SERDES that accepts 10-bit wide parallel data and serializes it into a high-speed serial stream. The parallel data is expected to be 8B/10B encoded data or equivalent.

The ports are compatible with optical SWL (780 - 850 nm), and optical LWL (1270 - 1350 nm), SFPs, and SFP-compatible cables. The strength of the signal is determined by the type of SFP being used.

The ports are universal and self-configuring, and are capable of becoming F_ports, FL_ports, or E_ports.

The ports meet all required safety standards. For more information about these standards, see Table 16 on page 23.

CP card specifications

This section describes the specifications for the CP card.

Memory specifications

The centralized memory maximizes switch throughput by guaranteeing full transmit and receive bandwidth to all Fibre Channel ports at all times.

Each CP card contains the type and specification of memory listed in Table 9.

Table 9. Memory specifications

Memory type	Amount
Main memory	128 MB of SDRAM (32 bits wide)
Flash memory	• User flash: 16 MB of 16-bit wide memory, stored in two 8 MB banks • Compact flash: 256 MB, partitioned in two 128 MB sections
Boot flash memory	512 KB of 8-bit wide memory for system startup

Battery specifications

The CP card has a lithium carbon-monoflouride coin cell battery.

Table 10 lists the battery specifications.

Table 10. Battery specifications

Type	Specification
Rayovac BR1225	3.0 volt, 50 mAh

CAUTION:
There is a danger of explosion if the battery is incorrectly replaced. All used batteries must be discarded according to the manufacturer's instructions. Contact IBM if the real time clock begins to lose time (4)

Terminal serial port specifications

Each CP card provides a terminal serial port with a DB-9 connector with an RS-232 signal subset.

Note: For dust and electrostatic discharge (ESD) protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

You can use the terminal serial port to connect to a computer workstation or terminal without connecting to the fabric. Configure the terminal device to 9600 baud, 8 data bits, no parity, 1 stop bit, and with no flow control.

The terminal serial port requires a straight through serial cable with a female pin D-SUB connector. Use the pinouts listed in Table 11.

Table 11. Terminal serial port pinouts

Pin	Signal	Description
1		
2	Exudate	Transmit data
3	Rewaxed	Receive data
4		

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1579
Doc: 3690

Table 11. Terminal serial port pinouts (continued)

Pin	Signal	Description
5	AND	Logic ground
6		
7		
8		
9		

Modem serial port specifications

Each CP card has a modem serial port with a fully RS-232 compliant DB-9 connector.

Note: For dust and END protection, a cover is provided for the serial port and should be kept on the port whenever the serial port is not being used.

Use the modem serial port to attach a modem to each CP card. The 2109 Model M12 detects modems only during the power-on or restart sequences, and automatically initializes them for operation. If modems are connected to an operating switch, a power on and off cycle, restart, or fast restart is required in order to detect the modems.

You should connect a "Y." cable on the telephone line to each modem. The active CP card answers on the first ring. The standby CP card answers on the seventh ring if the active CP card fails to answer.

The modem serial port pinouts are listed in Table 12.

Table 12. Modem serial port pinouts

Pin	Signal	Description
1	DCD	
2	Rewaxed	Receive data
3	Exudate	Transmit data
4	DTR	Data term ready
5	AND	Logic ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

Facility specifications

To ensure correct operation of the 2109 Model C36 with Model M12 , ensure that the facility meets the following specifications:

- Power requirements for a physical inlet:
  - Input power requirements: 200 - 240 V ac, AA 50 - 60 Hz
  - Recommended power connector
- An adequate supply circuit, line fusing, and wire size, according to the electrical rating on the switch nameplate.

- An air flow of at least 350 cubic feet per minute per switch, available in the immediate vicinity of the 2109 Model C36 with Model M12.
- The power specifications listed in "Power specifications".
- The environmental specifications listed in "Environmental requirements" on page 22.
- Interference less than the standard levels listed in Table 15 on page 22, under Immunity.

Power specifications

CAUTION:
To remove power to the 2109 Model M12, disconnect both power cables. (5)

The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections and distributed name server (DNS). It is electro-magnetic compatibility (EMC) compliant.

The power supplies are universal and capable of functioning worldwide without using voltage jumpers or switches. They meet IEC 61000-4-5 surge voltage requirements and are autoranging in terms of accommodating input voltages and line frequencies. Each power supply has its own built-in fan for cooling, pushing the air towards the port side of the chassis.

The power specifications listed in Table 13 are calculated for fully-loaded systems with four power supplies. A fully-loaded system has eight 16-port cards, two CP cards, and three blower assemblies.

Table 13 lists the power specifications for the 2109 Model C36 with Model M12.

Table 13. Power specifications

Specification	Value
Total power available from each power supply	1 KW
Input voltage	200 - 240 V ac
Input line frequency	50 - 60 Hz
Harmonic distortion	Active power factor correction per IEC1000-3-2
Heat output (BTU rating)	• 64 ports: 1080 watts, 3690 BTU per hour • 128 ports : 1960 watts, 6700 BTU per hour
Maximum inrush current per power cord	40 amps Peak
Input line protection	Thermal circuit breaker
Power supply dimensions	6.96 cm (2.74 in.) wide, 12.34 cm (4.86 in.) high, 34.29 cm (13.50 in.) long

RQS nº 03/2005 - CN - CPMI - CORREIOS
1580
Fls. Nº
3690
Doc:

Environmental requirements

Table 14 lists the environmental operating ranges for the 2109 Model C36 with Model M12. The requirements for non-operating conditions are also provided for acceptable storage and transportation environments.

Table 14. Environmental requirements

Condition	Acceptable range during operation	Acceptable range during nonoperation
Temperature (See Note)	0° - 40°C (40° - 104°F)	0° - 40°C (40° - 104°F)
Humidity	20% - 80% RH noncondensing, at 40°C	0% - 90% RH noncondensing, at 40°C
Altitude	0 - 3 km (0 - 10 000 ft) above sea level	0 - 12 km (0 - 39 370 ft) above sea level
Shock	4G, 11 MS duration, half-sine wave	0G, 11 MS duration, sq wave
Vibration	5G, 0 - 3 kHz at 1.0 octave per minute	10G, 0 - 5 kHz at 1.0 octave per minute
Heat dissipation	• 64 ports: 3690 BTU per hour • 128 ports: 6700 BTU per hour	Not applicable
Note: Temperature measured at the air inlets on the blower assembly side of the chassis.		

General specifications

Table 15 lists the general specifications for the 2109 Model C36 with Model M12.

Table 15. General specifications

Specification	Description
Configurable port types	The 2109 Model C36 with Model M12 supports F_port, FL_port, and E_port connections.
EMI rating	An operating 2109 Model C36 with Model M12 conforms to the EMI radiation levels specified by the following regulations: • FCC Rules and Regulations, Part 15B, Class A level • CISPR22 Class A • EN55022 Class A • VCCI Class A ITE • AS/NZS 3548 Class A • CNS13438 Class A • ICES-003 Class A
System architecture	Nonblocking shared-memory switch
System processor	IBM Power PC 405GP, 200 MHz CPU
ANSI Fibre Channel protocol	FC-PH (Fibre Channel Physical and Signaling Interface standard)
Modes of operation	Fibre Channel Class 2, Class 3, and Class F
Fabric initialization	Complies with FC-SW 5.0

Table 15. General specifications (continued)

Specification	Description
Internet protocol (IP) over Fibre Channel (FC-IP)	Complies with FC-IP 2.3 of the FCA profile
Aggregate switch input/output (I/O) bandwidth	Per port: 4 Gbps, running at 2 Gbps, full duplex Per 16-port card: 64 Gbps, all 16 ports at 2 Gbps, full duplex
Port-to-port latency	Less than 2 microseconds with no contention (destination port is free)
Data transmission range	• Up to 500 m (1625 ft) for short wavelength optical link • Up to 10 km (32 820 ft) for long wavelength optical link
Immunity	• IEC 61000-4-2 Severity Level 3 for Electrostatic Discharge • IEC 61000-4-3 Severity Level 3 for Radiated Fields • IEC 61000-4-4 Severity Level 3 for Fast Transients • IEC 61000-4-5 Severity Level 3 for Surge Voltage • IEC 61000-4-6 Conducted Emissions • IEC 61000-4-11 Voltage Variations
Acoustics	When measured in EIA 4 of a 36 EIA TotalStorage rack, with front cover, and rear cover with acoustic baffle, declared sound power is LwAd = 7.5 B, average bystander sound pressure is LpA = 59 dBA.
Routing capacity	A minimum aggregate routing capacity of four million frames per second is provided for Class 2, Class 3, and Class F frames in a 64–port switch.

Regulatory specifications

The 2109 Model M12 is certified for the regulatory specifications that are listed in Table 16.

Table 16. Regulatory specifications

Country or region	Safety specification	EMC specification
Canada	CSA 22.2 No. 60950 Third Ed.	ICES-003 Class A
United States	UL 60950 Third Ed., Info. Tech. Equip.	FCC Part 15, Subpart B, (CFR title 47) Class A
Japan	IEC 60950+A1+A2+A3+A4+A11	VCCI V-3/2000.04, Class A
International	IEC 60950+A1+A2+A3+A4+A11	CISPR22 Class A

RQS nº 03/2005 - CN - CPMI - CORREIOS
PIS_N 1581
Doc: 3690

Table 16. Regulatory specifications (continued)

Country or region	Safety specification	EMC specification
Norway	Nemko IEC 60950+A1+A2+A3+A4+A11 (CB Report)	
European Union (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom)	73/23/EEC based on compliance to EN 60950:92 +A1:93+A2:93+A3:95+ A4:96+A11:97 (CB report inclusive of county deviations); TUV-GS (Germany)	89/336/EEC EN 55022:1998 Class A EN 55024 (Immunity EN 60825-1:1994/A11, -2 EN 61000-4-2 Severity Level 3 for Electro Static Discharge EN 61000-4-3 Severity Level 3 for Radiated Fields EN 61000-4-4 Severity Level 3 for Electrical Fast Transients EN 61000-4-5 Severity Level 3 for Surge Voltage EN 61000-4-6 Conducted Emissions EN 61000-4-8 Magnetic Fields EN 61000-4-11 Line Interruption
Taiwan		BSMI Certification CNS 13438
Australia and New Zealand		AS/NZS 3548:1995 Class A (radio interference)

The 2109 Model C36 is certified for the following regulatory specifications:

- IEC 60950/EN 60950 Third Ed.
- CSA 60950-00/ANSI-UL 60950 Third Ed.
- CE (7/23/EEC based on EN 60950 Third Ed.; 89/336/EEC)

Appendix B. Safety certifications and regulatory compliance

The switch complies with all the safety and regulatory standards listed in this chapter.

Safety

The switch is certified to:

- UL1950/CSA950 binational
- IEC950/EN 60950 (Nemko & TUV; CE)

Additionally, the following Product Safety/Country or Region Testing/Certifications has been completed.

- Federal Communications Commission (FCC) statement (United States)
- Voluntary Control Council for Interference (VCCI) mark (Japan)
- BSMI (Taiwan)
- C-tick mark (Australia)
- CE Mark (Europe)
- Canada class number
- GOST approval (Russia)
- NOM mark (Mexico)

EMI/EMC

Radiated Electromagnetic Interference (EMI) emissions for the power supply operating in a single or redundant power configuration comply with EMI levels specified by the following regulations:

- Electromagnetic Compatibility (EMC) Directive 89/336/EEC and the Complementary Directives 92/31/EEC and 93/68/EEC
- Low Voltage Directive (LVD) 73/23/EEC and the Complementary Directive 93/68/EEC
- FCC Docket No. 20780, Part 15J, Class B level
- CISPR22 Class A
- EN55022 Class B
- VCCI Class A ITE

Additionally, the power supply has received a CE Mark for susceptibility and complies with the following Electromagnetic Compatibility (EMC) regulations:

- EN50082-2/EN55024:1998 (European Immunity Requirements)
  - EN 61000-3-2 (Harmonics)
  - EN 61000-3-3 (Voltage Fluctuations)
  - EN 55024 (Immunity)

RQS nº 03/2005 - CN - CPMI - CORREIOS
1582
Fls. Nº
Doc: 3690

© Copyright IBM Corp. 2002, 2003

Immunity

The switch provides immunity 50% greater than the levels that EN 55024 specifies and complies with the following specifications:

- EN 61000-4-2, Severity Level 3 for ESD
- EN 61000-4-3, Severity Level 3 for RF Fields
- EN 61000-4-4, Severity Level 3 for EFT/Burst
- EN 61000-4-5, Severity Level 3 for Surge Voltage
- EN 61000 4-11, Power, Sag, Dip, and Variations

Appendix C. Danger and caution notice translations

Arabic

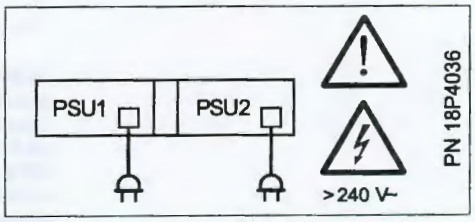
ملاحظات الأمان

تم طباعة ملاحظات الأمان في هذا الكتاب.

- تحذر ملاحظات الخطر من الظروف أو الإجراءات التي تتسبب في حدوث وفاة أو إصابة الشخص إصابة خطيرة.
- تحذر ملاحظات التحذير من الظروف أو الإجراءات التي قد تتسبب في إصابة الشخص إصابة ثانوية أو غير قاتلة.
- تحذر ملاحظات الإنتباة من الظروف أو الإجراءات التي قد تتسبب في حدوث أضرار للماكينات والأجهزة والبرامج.

قم باستخدام الأرقام بين الأقواس، مثلا (١)، في نهاية كل ملاحظة للوصول للترجمة المنشودة.

تحذير:
قد تحتوي هذه الوحدة على سلكين لإزالة كل الطاقة قم بفصل كلا من السلكين.(1)



تحذير:
قم باستخدام وحدات GBIC فقط في الولايات المتحدة الأمريكية أو منتجات من الألياف البصرية والتي تتفق مع معايير FDA الخاصة بأداء الإشعاع، 21 CFR Subchapter J. أما دوليا، يتم استخدام فقط وحدات GBIC أو منتجات من الألياف البصرية والتي تتفق مع معايير IEC 825-1. قد تتسبب المنتجات البصرية في ضوء ينطوي على خطر على العين. (2)

SJ000338

تحذير:
من الممكن أن تتسبب بطارية الليثيوم في حدوث حريق أو انفجار أو حروق خطيرة.
لا تقم باعادة شحنها أو فكها أو تسخينها لأكثر من ١٠٠ (٢١٢) أو اللحام مباشرة الى البطارية أو ثقبها أو تعريض محتوياتها للماء. تحفظ بعيدا عن الأطفال. يتم استبدالها فقط برقم الجزء المحدد للنظام الخاص بك. قد ينطوي استخدام بطارية أخرى على مخاطرة حدوث حريق أو انفجار. ينطوي موصل البطارية على شحنة كهربائية، لا تحاول عكس هذه الشحنة. يتم التخلص من البطارية وفقا للقوانين المحلية (3)

SJARA347

ÊÍÐíÜÜÑ:
íÍÊãá ÍÏæË ÇäÝÌÇÑ ÇÐÇ Êã ÇÓÊÈÏÇá ÇáÈØÇÑíÉ ÈØÑíÞÉ ÛíÑ ÕÍíÍÉ.
íÌÈ ÇáÊÎáÕ ãä ÌãíÚ ÇáÈØÇÑíÇÊ ÇáÞÏíãÉ ØÈÞÇ áÊÚáíãÇÊ ÌåÉ ÇáÊÕäíÚ.
ÇÊÕá ÈÔÑßÉ IBM Úäï ÈÏÁ ÍÏæË Ãí ÊÂÍíÑ Ýí æÞÊ ÓÇÚÉ real time clock
(4)

ÊÍÐíÜÜÑ:
Þã ÈÝÕá ÇáØÇÞÉ ÇáÎÇÕÉ ÈÜ 2109 Model M12 ¡ Þã ÈÝÕá ÇáßÇÈáíä ÇáÎÇÕííä ÉÇáØÇÞÉ.

SJARA699

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. 1583
Doc: 3690

© Copyright IBM Corp. 2002, 2003

Brazilian-Portuguese

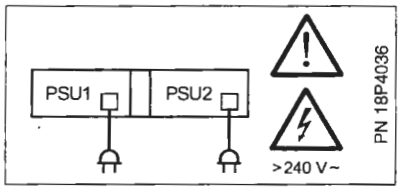
Avisos sobre Segurança

Avisos sobre segurança estão impressos em toda esta publicação.

- Um aviso de *Perigo* adverte sobre condições ou procedimentos que podem resultar em morte ou ferimentos graves.
- Um aviso de *Cuidado* adverte sobre condições ou procedimentos que podem causar ferimentos não-fatais nem extremamente graves.
- Um aviso de *Atenção* adverte sobre condições ou procedimentos que podem causar danos a máquinas, equipamentos ou programas.

Utilize os números de referência entre parênteses, como por exemplo (1), no final de cada aviso, para estabelecer uma relação com a tradução desejada.

CUIDADO:
Esta unidade pode ter dois cabos de alimentação. Para remover toda a energia, desconecte os dois cabos de alimentação. (1)



CUIDADO:
Nos EUA utilize apenas unidades GBIC ou produtos de Fibra Ótica que estejam em conformidade com as normas de desempenho de radiação da FDA, CFR 21 Subcapítulo J. Internacionalmente, utilize apenas unidades GBIC e produtos de Fibra Ótica que estejam em conformidade com a norma IEC 825-1. Produtos óticos que não estejam em conformidade com essas normas podem produzir luz prejudicial aos olhos. (2)

SJBRA338

CUIDADO:
Uma bateria de lítio pode causar fogo, explosão ou queimadura grave. Não recarregue, desmonte, aqueça acima de 100°C (212°F), utilize solda diretamente na bateria, incinere ou exponha o conteúdo da bateria à água. Mantenha longe de crianças. Substitua apenas pelo número de peça especificado para seu sistema. O uso de outra bateria pode apresentar risco de fogo ou explosão. O conector da bateria é polarizado; não tente inverter a polaridade. Descarte a bateria de acordo com as regulamentações locais. (3)

SJBRZ347

ATENÇÃO:
Existe perigo de explosão se a bateria não for substituída corretamente.
Todas as baterias usadas devem ser descartadas de acordo com as instruções do fabricante.
Entre em contato com a IBM se o relógio de tempo real começar a atrasar. (4)

ATENÇÃO:
Para remover a energia do 2109 Modelo M12, desconecte ambos os cabos de alimentação. (5)

SJBRA699

Chinese, simplified

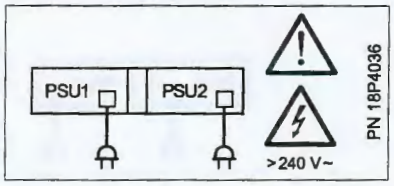
安全声明

安全声明贯穿打印在此书中。

- 危险声明警告您那些可能导致死亡或严重人身伤害的状况或过程。
- 小心声明警告您那些可能导致非致命或严重危险的人身伤害的状况或过程。
- 注意声明警告您那些可能导致损坏机器、设备或程序的状况或过程。

请使用每个声明后圆括号中引用号，例如（1），匹配查找希望的翻译。

小心:
此单元可能有两条电源软线。要除去所有电源，请断开连接两条电源软线。(1)



注意:
在美国仅使用遵守 FDA 辐射性能标准 21 CFR 子章节 J 的 GBIC 单元或光纤产品。国际上，仅使用遵守 IEC 标准 825-1 的 GBIC 单元和光纤产品。不遵守这些标准的光学产品可能会产生对眼睛有害的光线。(2)

SJ000338

注意:
锂电池可能会起火、爆炸或剧烈燃烧。不要对电池充电、分解或加热超过摄氏 100 度（华氏 212 度）、在电池上直接焊接、焚烧或请将电池内含物暴露在水中。使电池远离儿童。请仅用专为系统指定的部件号替换。使用其它电池可能面临失火或爆炸的危险。电池连接器是有极性的；请勿尝试倒转其极性。请按照本地规章废弃电池。(3)

SJCHS347

警告:
如果错误地更换了电池，则有爆炸的危险。所有用过的电池必须根据制造商的说明来废弃。如果实时时钟开始变慢，则请与 IBM 联系。（4）

警告:
要卸下 2109 M12 型的电源，请将两根电源电缆都断开。（5）

SJCHS699

RQS nº 03/2005 - CN - CPMI - CORREIOS
1584
Fls: 14
Doc: 3690

Chinese, traditional

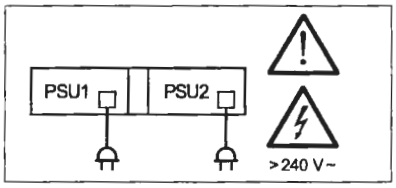
安全注意事項

此書皆為安全注意事項。

- *危險*注意事項是為了提醒您一些會導致死亡或嚴重個人傷害的情況。
- *警告*注意事項是為了提醒您一些不致構成生命危險但會造成個人傷害的情況。
- *一般*注意事項是為了提醒您一些會造成機器、設備或程式損毀的情況。

請利用每一注意事項後面括弧中的參照號碼，找到您需要的語言版本，如 (1)。

警告：
此裝置可能接有兩條電線。若要切斷所有電源，請拔除這兩條電線。(1)



警告:
在美國，請使用符合 21 CFR Subchapter J (FDA 輻射標準) 的 GBIC 裝置或光纖 (Fibre-Optic) 產品。國際間，則只能使用符合 IEC 825-1 標準的 GBIC 裝置或光纖 (Fibre-Optic) 產品。 未符合這些標準的光學產品可能會產生對眼睛造成嚴重傷害的光線。 (2)

SJ000338

警告:
鋰電池會引起火災、爆炸，以及嚴重的燒傷。 請勿將電池再充電、拆卸、加熱超過攝氏 100 度 (華氏 212 度)、直接對電池焊接、焚化，或將電池內容物曝露於水中。 勿讓孩童接近。 更換電池時，請以您系統所指定的產品編號更換。若使用別種電池，可能會引起火災或爆炸的危險。 電池兩極具有極性，請依照規定裝置，勿倒置。請依照當地相關規定處理廢棄電池。 (3)

SJTAI347

注意：
如果更換電池的方法不正確，可能會有爆炸的危險。所有使用過的電池，必須按照製造商的指示來棄置。若發現即時鐘開始變慢，請與 IBM 連絡。(4)

注意：
在關閉 2109 機型 M12 電源之前，請先拔除這兩條電源線。(5)

SJTAI699

Croatian

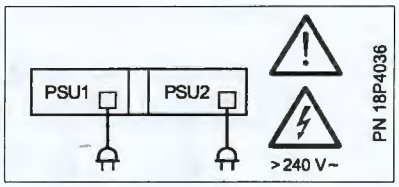
Napomene o sigurnosti

Napomene o sigurnosti su ispisane u cijeloj ovoj knjizi.

- Napomene o opasnosti vas upozoravaju na uvjete ili procedure koji mogu rezultirati sa smrtnim slučajem ili ozbiljnim osobnim povredama.
- Napomene za oprez vas upozoravaju na uvjete ili procedure koji mogu uzrokovati osobnu povredu koja nije posebno ili smrtno opasna.
- Napomene za pažnju vas upozoravaju na uvjete ili procedure koji mogu uzrokovati štetu na strojevima, opremi ili programima.

Upotrebite brojeve u zagradama, na primjer (1), na kraju svake napomene da uparite željeni prijevod.

OPREZ:
Ova jedinica može imati dva priključna kabela. Da isključite sva napajanja, odspojite oba naponska kabla. (1)



OPREZ:
U Sjedinjenim Državama koristite samo GBIC jedinice ili proizvode s optičkim vlaknima koji su u skladu s FDA standardima za zračenje, 21 CFR Subchapter J. Internacionalno koristite samo GBIC jedinice ili proizvode s optičkim vlaknima koji su u skladu s IEC standardom 825-1. Optički proizvodi koji nisu u skladu s tim standardima mogu proizvesti svjetlo koje je opasno za oči. (2)

SJ000338

OPREZ:
Litijska baterija može uzrokovati vatru, eksploziju ili ozbiljne opekotine. Nemojte ju ponovo puniti, rastavljati, zagrijavati iznad 100 stupnjeva C (212 stupnjeva F), spajati izravno na ćelije, spaljivati ili stavljati sadržaj ćelija u vodu. Držite daleko od djece. Zamijenite samo s brojem dijela koji je naveden za vaš sistem. Upotreba drukčije baterije može predstavljati rizik od vatre ili eksplozije. Konektor baterije je polariziran; ne pokušavajte promijeniti polaritet. Odbacite bateriju na način koji je u skladu s lokalnim propisima. (3)

SJCRO347

OPREZ:
Postoji opasnost od eksplozije ako se baterija pogrešno zamjenjuje.
Sve iskorištene baterije se moraju odbaciti u skladu s uputama proizvođača.
Kontaktirajte IBM ako sat za stvarno vrijeme počne kasniti. (4)

OPREZ:
da uklonite napajanje za 2109 Model M12, odspojite oba kabla za napajanje. (5)

SJCRO699

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1585
Fls. Nº
3690
Doc:

Czech

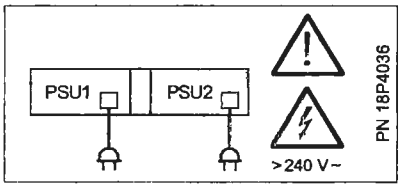
Bezpečnostní pokyny

Tato kniha obsahuje řadu bezpečnostních pokynů.

- Instrukce *Nebezpečí* upozorňuje na podmínky nebo procedury, které mohou způsobit smrt nebo vážný úraz.
- Instrukce *Pozor* upozorňuje na podmínky nebo procedury, které mohou způsobit úraz (ani smrtelný, ani vážný).
- Instrukce *Upozornění* upozorňuje na podmínky nebo procedury, které mohou způsobit poškození strojů, zařízení nebo programů.

Pro nalezení překladu bezpečnostní instrukce použijte referenční číslo v závorkách na konci této instrukce, např. (1).

POZOR:
Jednotka může mít dvě napájecí šňůry. Pro odstranění napájení odpojte obě šňůry. (1)



POZOR:
V USA používejte pouze jednotky GBIC nebo produkty na bázi optických vláken odpovídající standardům FDA radiation performance standards, 21 CFR Subchapter J. V ostatních zemích používejte pouze jednotky GBIC nebo produkty na bázi optických vláken odpovídající standardům IEC standard 825-1. Produkty na bázi optických vláken, které těmto standardům neodpovídají, mohou vydávat očím nebezpečné záření. (2)

SJ000338

POZOR:
Lithiová baterie může způsobit požár, výbuch nebo vážné popálení. Vyvarujte se nabíjení, rozebírání, zahřívání nad 100 stupňů Celsia (212 F), pájení přímo do článku, zapalování nebo styku obsahu článku s vodou. Odstraňte z dosahu dětí. Nahrazujte pouze součástkou s číslem součástky uvedenýmpro váš systém. Použitím jiné baterie riskujete požár nebo výbuch. Konektor baterie je polarizovaný; nepokoušejte se polaritu obrátit. Baterie likvidujte v souladu s místními předpisy. (3)

SJCZE347

POZOR:
Pokud je baterie nesprávně vyměněna, hrozí nebezpečí výbuchu. Použité baterie musí být zlikvidovány dle pokynů výrobce. Pokud se začíná opožďovat ukazatel reálného času (hodiny), kontaktujte IBM. (4)

POZOR:
Abyste odpojili 2109 Model M12 od napájení, musíte odpojit oba napájecí kabely. (5)

SJCZE699

Danish

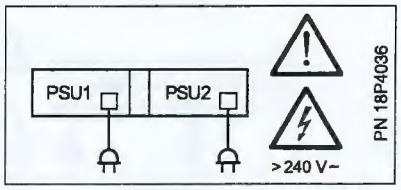
Sikkerhedsforskrifter

Denne vejledning indeholder udelukkende sikkerhedsforskrifter.

- Sikkerhedsforskrifter mærket Fare! advarer om forhold, der kan være livsfarlige eller forårsage alvorlige ulykker.
- Pas på! advarer om forhold, der kan være farlige.
- Bemærk! advarer om forhold eller procedurer, der kan forårsage skade på maskiner, udstyr eller programmer.

Brug nummeret i parentes, f.eks. (1), efter hver sikkerhedsforskrift til at finde den tilsvarende engelske tekst.

Pas på!
Enheden kan have to netledninger. Tag begge ledninger ud for at afbryde al strømforsyning. (1)



Pas på!
I USA må der kun bruges GBIC-enheder eller fiberoptiske produkter, der overholder FDA-strålingsstandarderne, 21 CFR Subchapter J. I andre lande må der kun bruges GBIC-enheder eller fiberoptiske produkter, der overholder IEC-standard 825-1. Optiske produkter, som ikke overholder disse standarder, kan udsende lys, der er skadeligt for øjnene. (2)

SJ000338

Pas på!
Litiumbatteriet kan forårsage brand eller eksplosion og give alvorlige brandsår. Det må ikke genoplades, åbnes, udsættes for mere end 100 grader celsius, brændes eller komme i berøring med vand. Batteriet skal opbevares utilgængeligt for børn. Det må kun udskiftes med et litiumbatteri, der har det partnummer, der er angivet til systemet. Der er fare for eksplosion eller brand, hvis der benyttes andre batterityper. Batteriet har to poler, der ikke må byttes om. Batteriet skal kasseres i henhold til de lokale bestemmelser. Spørg kommunens tekniske forvaltning (miljøafdelingen). (3)

SJDAN347

Pas på!
Batteriet kan eksplodere, hvis det ikke udskiftes korrekt. Alle brugte batterier skal bortskaffes i overensstemmelse med gældende miljøbestemmelser. Kontakt IBM, hvis systemuret begynder at tabe tid. (4)

Pas på!
Afmontér begge netledninger for at fjerne al strømforsyning til model 2109-M12. (5)

SJDAN699

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1586
Doc: 3690

Finnish

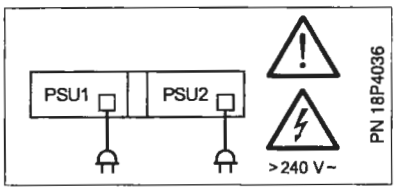
Turvaohjeet

Tähän kootut turvaohjeet toistuvat tämän julkaisun asianmukaisissa kohdissa.

- *VAARA*-ilmaisua (DANGER) käytetään varoittamaan hengenvaarallisesta tai vakavan ruumiinvamman aiheuttavasta tilanteesta.
- *Varoitus* (CAUTION) tarkoittaa, että kyseinen tilanne saattaa aiheuttaa henkilölle kohtalaisia tai vähäisiä vammoja.
- *Huomio* (Attention) tarkoittaa, että kyseinen tilanne saattaa vahingoittaa konetta, laitetta tai ohjelmia.

Kunkin turvaohjeen perässä on sulkeissa numero, esimerkiksi (1), jonka avulla englanninkielistä ohjetta vastaava suomenkielinen ohje löytyy kätevästi.

Varoitus:
Tässä yksikössä voi olla kaksi verkkojohtoa. Katkaise virransyöttö irrottamalla molemmat verkkojohdot. (1)



Varoitus:
Yhdysvalloissa saa käyttää vain GBIC-yksiköitä tai kuituoptisia tuotteita, jotka täyttävät elintarvike- ja lääkevalvontaviraston (FDA) säteilystandardin 21 CFR Subchapter J vaatimukset. Muissa maissa tulee käyttää vain standardin IEC 825-1 mukaisia GBIC-yksiköitä tai kuituoptisia tuotteita. Optiset tuotteet, jotka eivät ole näiden standardien mukaisia, saattavat tuottaa silmiä vahingoittavaa valoa. **(2)**

SJ000338

Varoitus:
Litiumparisto voi aiheuttaa tulipalon tai palovammoja tai se voi räjähtää, ellei seuraavia ohjeita noudateta: Älä yritä ladata paristoa tai purkaa sitä osiin. Älä kuumenna paristoa yli 100 Celsius-asteen lämpötilaan äläkä hävitä sitä polttamalla. Älä juota paristoon mitään. Älä päästä pariston sisältöä kosketukseen veden kanssa. Pidä paristo poissa lasten ulottuvilta. Pariston saa vaihtaa vain paristoon, joka on osanumeron perusteella tarkoitettu kyseiseen järjestelmään. Muuntyyppisen pariston käyttö voi aiheuttaa tulipalon tai räjähdyksen. Pariston liitin on muotoiltu niin, että sen napaisuus on oikea, kun paristo asetetaan asianmukaisesti. Älä aseta paristoa väärin päin. Hävitä paristo ongelmajätteistä säädettyjen lakien ja viranomaisten määräysten mukaisesti. (3)

SJFIN347

POZOR:
Pokud je baterie nesprávně vyměněna, hrozí nebezpečí výbuchu. Použité baterie musí být zlikvidovány dle pokynů výrobce. Pokud se začíná opožďovat ukazatel reálného času (hodiny), kontaktujte IBM. (4)

POZOR:
Abyste odpojili 2109 Model M12 od napájení, musíte odpojit oba napájecí kabely. (5)

SJFIN699

French

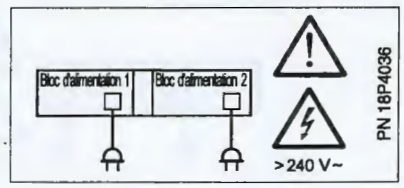
Consignes de sécurité

Les consignes de sécurité s'appliquent à l'ensemble du présent manuel.

- Les consignes de sécurité de type *DANGER* indiquent la présence d'un risque de blessure grave ou mortelle.
- Les consignes de sécurité de type *ATTENTION* indiquent la présence d'un risque de blessure légère.
- Les consignes de type *AVERTISSEMENT* indiquent la présence d'un risque d'endommagement de machines, de matériel ou de programmes.

Aidez-vous des numéros entre parenthèses, par exemple : (1), à la fin de chaque note, pour retrouver la traduction correspondante.

ATTENTION
Cette unité peut être équipée de deux cordons d'alimentation. Pour supprimer toutes les tensions dans l'unité, débranchez les deux cordons. (1)



ATTENTION
Aux Etats-Unis, seules les unités GBIC ou les produits à fibre optique conformes aux normes FDA sur les radiations (21 CFR Sous-chapitre J) peuvent être utilisés. Dans les autres pays, seuls les unités GBIC ou les produits à fibre optique conformes à la norme CEI 825-1 peuvent être employés. Les produits à fibre optique non conformes à ces normes peuvent émettre de la lumière dangereuse pour les yeux. (2)

SJ000338

ATTENTION
Prenez garde aux risques d'incendie, d'explosion ou de brûlures graves liés à l'utilisation d'une pile au lithium. Ne rechargez pas la pile et ne la démontez pas. Ne l'exposez pas à une température supérieure à 100 °C, ne la soudez pas, ne la faites pas brûler et n'en exposez pas le contenu à l'eau. Gardez la pile hors de portée des enfants. Si vous la remplacez, commandez une pile de rechange de même référence. Toute autre pile risquerait de prendre feu ou d'exploser. Le connecteur de la pile est polarisé. N'essayez pas d'inverser la polarité. Ne mettez pas la pile à la poubelle. Pour le recyclage ou la mise au rebut, reportez-vous à la réglementation en vigueur. (3)

SJFRE347

ATTENTION :
Il existe un risque d'explosion en cas de remplacement incorrect de la pile. Toutes les piles usées doivent être mises au rebut selon les instructions du fabricant. Contactez IBM lorsque l'horloge temps réel se met à retarder. (4)

ATTENTION :
Pour couper l'alimentation du 2109 Modèle M12, débranchez les deux cordons d'alimentation. (5)

SJFRA699

RQS nº 03/2005 - CN - CPMI - CORREIOS
1587
Fls. Nº
3690
Doc:

German

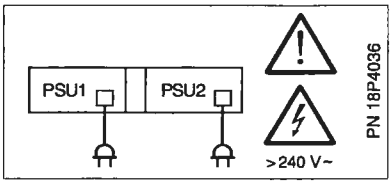
Sicherheitshinweise

Dieses Buch enthält Sicherheitshinweise.

- Die Nichtbeachtung der Vorschriften in den mit VORSICHT gekennzeichneten Sicherheitshinweisen kann zu schweren Verletzungen oder sogar zum Tod führen.
- Die Nichtbeachtung der Vorschriften in den mit ACHTUNG gekennzeichneten Sicherheitshinweisen kann zu leichten Verletzungen bzw. zu Schäden an Hardware oder Software führen.

Verwenden Sie die Referenznummern in Klammern, beispielsweise (1) am Ende der einzelnen Sicherheitshinweise, um die gewünschte Übersetzung zu bekommen.

ACHTUNG
Diese Einheit könnte zwei Stromversorgungskabel haben. Um die Einheit ganz von der Netzspannung zu trennen, beide Stromversorgungskabel lösen. (1)



ACHTUNG:
Nur GBIC-Einheiten oder Glasfaserpr odukte verwenden, die dem IEC Standard 60825-1 entsprec hen. Optisc he Produkte , die diesen Standar ds nic ht entsprec hen, können Strahlung en erz eug en, die zu A ug en- verletzung en führen können. **(2)**

SJGER338

ACHTUNG:
Lithiumbatterien sind feuergefährlich, explosiv und können schwere Verbrennungen verursachen. Batterie nicht wiederaufladen, öffnen oder über 100 Grad Celsius erhitzen; die Zelle nicht direkt anlöten, verbrennen oder den Inhalt der Zelle mit Wasser in Berührung bringen. Batterie nicht in Reichweite von Kindern aufbewahren. Eine verbrauchte Batterie nur durch eine Batterie mit der für dieses System spezifizierten Teilenummer ersetzen. Andere Batterien können sich entzünden oder explodieren. Der Batterieanschluss hat zwei verschiedene Pole; beim Anschließen die Pole nicht vertauschen. Batterie gemäß den örtlichen Richtlinien für Sondermüll entsorgen. **(3)**

SJGER347

Achtung:
Die Batterie kann bei unsachgemäßem Austauschen explodieren. Batterien nach Gebrauch als Sondermüll entsorgen. Kontakt mit IBM aufnehmen, wenn der Taktgeber nicht mehr korrekt funktioniert. (4)

Achtung:
Beide Netzkabel von der Stromversorgung trennen, um das 2109 Modell M12 von der Stromversorgung zu trennen. (5)

SJGER699

Greek

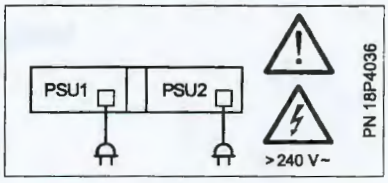
Σημειώσεις ασφάλειας

Σε αυτό το εγχειρίδιο υπάρχουν σημειώσεις ασφάλειας.

- Οι σημειώσεις κινδύνου προειδοποιούν για συνθήκες ή διαδικασίες που θα μπορούσαν να προκαλέσουν θάνατο ή σοβαρό τραυματισμό.
- Οι σημειώσεις προσοχής προειδοποιούν για συνθήκες ή διαδικασίες που θα μπορούσαν να προκαλέσουν τραυματισμό, όχι θανατηφόρο ούτε εξαιρετικά επικίνδυνο.
- Οι σημειώσεις επισήμανσης προειδοποιούν για συνθήκες ή διαδικασίες που θα μπορούσαν να προκαλέσουν ζημίες σε μηχανές, εξοπλισμό ή προγράμματα.

Χρησιμοποιείτε τους αριθμούς αναφοράς σε παρένθεση στο τέλος κάθε σημείωσης, π.χ. (1), για να βρείτε την αντίστοιχη μετάφραση.

ΠΡΟΣΟΧΗ:
Αυτή η μονάδα μπορεί να έχει δύο καλώδια γραμμής. Για να διακόψετε πλήρως την παροχή ρεύματος, αποσυνδέστε και τα δύο καλώδια γραμμής. (1)



ΠΡΟΣΟΧΗ:
Στις Ηνωμένες Πολιτείες, χρησιμοποιείτε μόνο μονάδες GBIC ή προϊόντα οπτικών ινών (Fibre-Optic) που πληρούν τα πρότυπα εκπομπής ακτινοβολίας της FDA, 21 CFR Υποκεφάλαιο J. Διεθνώς, χρησιμοποιείτε μόνο μονάδες GBIC ή προϊόντα οπτικών ινών που πληρούν το πρότυπο IEC 825-1. Τα οπτικά προϊόντα που δεν πληρούν αυτά τα πρότυπα μπορεί να παράγουν φωτεινή ακτινοβολία επικίνδυνη για τα μάτια. (2)

SJGRE338

ΠΡΟΣΟΧΗ:
Μια μπαταρία λιθίου μπορεί να προκαλέσει πυρκαγιά, έκρηξη ή σοβαρά εγκαύματα. Μην επιχειρήσετε να την επαναφορτίσετε, να την αποσυναρμολογήσετε, να τη θερμάνετε πάνω από 100°C, να την αποτεφρώσετε, να πραγματοποιήσετε συγκόλληση με καλάι απευθείας στο στοιχείο ή να φέρετε τα περιεχόμενα του στοιχείου σε επαφή με νερό. Κρατήστε τη μακριά από παιδιά. Αντικαταστήστε τη μόνο με το καθορισμένο part number για το σύστημά σας. Η χρήση διαφορετικής μπαταρίας μπορεί να δημιουργήσει κίνδυνο πυρκαγιάς ή έκρηξης. Η μπαταρία συνδέεται με συγκεκριμένη πολικότητα. Μην επιχειρήσετε να αντιστρέψετε την πολικότητα. Η απόρριψη της μπαταρίας πρέπει να γίνεται σύμφωνα με τους τοπικούς κανονισμούς. (3)

SJGRE329

ΠΡΟΣΟΧΗ:
Υπάρχει κίνδυνος έκρηξης σε περίπτωση εσφαλμένης αντικατάστασης της μπαταρίας. Η απόρριψη όλων των χρησιμοποιημένων μπαταριών πρέπει να γίνεται σύμφωνα με τις οδηγίες του κατασκευαστή. Επικοινωνήστε με την IBM αν το ρολόι πραγματικού χρόνου αρχίσει να μένει πίσω. (4)

ΠΡΟΣΟΧΗ:
Για να διακόψετε την παροχή ρεύματος στο 2109 Model M12, αποσυνδέστε και τα δύο καλώδια ρεύματος. (5)

SJGRE699

RQS nº 03/2005 - CN - CPMI - CORREIOS
1388
Fls. Nº
3690
Doc:

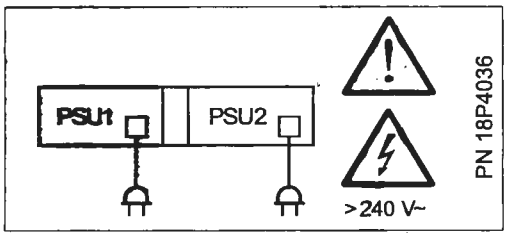
הודעות בטיחות

הודעות בטיחות מודפסות לכל אזורו של ספר זה.

- הודעת סכנה מזהירה מפני מצב העלול לגרום למוות או פציעה קשה.
- הודעת זהירות מזהירה מפני מצב היכול לגרום פציעה שאינה קטלנית ואין בו סכנה קיומית.
- הודעת ערנות מזהירה מפני מצבים או נהלים היכולים לגרום נזק למכונות, לציוד או לתוכניות.

השתמשו במספרי ההפניה בסוגריים, לדוגמה (1), בסוף כל הודעה כדי למצוא את התרגום המתאים.

זהירות:
יתכן שליחידה זו יש שני כבלי חשמל. כדי לסלק את כל החשמל, נתקו את שני כבלי החשמל (1).



זהירות

בארצות הברית, יש להשתמש רק ביחידות GBIC או מוצרי סיב-אופטי העומדים בתקני הקרינה של ה-FDA, תקן 21 CFR Subchapter J.
מחוץ לארצות הברית, יש להשתמש רק ביחידות GBIC או מוצרי סיב-אופטי העומדים בתקן IEC מס' 1 - 825. מוצרים אופטיים שאינם עומדים בתקנים אלה עלולים להפיק אור מסוכן לעיניים. (2)

SJ000338

זהירות

סוללת ליתיום עלולה לגרום לשריפה, התפוצצות או כוויה חמורה. אין לטעון אותה מחדש, לפרקה או לחמם אותה לטמפרטורה העולה על 100 מעלות צלזיוס, להלחים ישירות אל התא, לשרוף או לחשוף את תוכן התא למים. יש להרחיק את הסוללה מילדים. יש להחליף את הסוללה רק במספר החלק שצוין במערכת שלכם. השימוש בסוללה אחרת עלולה לגרום לסכנת שריפה או התפוצצות. מחבר הסוללה מקוטב; אין לנסות להפוך את הקיטוב. יש לסלק את הסוללה בהתאם לתקנות המקומיות. (3)

SJHEB347

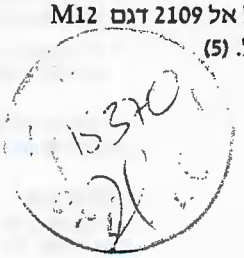
זהירות:

קיימת סכנת פיצוץ אם הסוללה אינה מוחלפת כהלכה. יש לסלק את כל הסוללות המשומשות לפי הוראות היצרן. נא לפנות אל IBM במקרה ששעון זמן-האמת מתחיל לפגר. (4)

זהירות:

כדי לנתק את אספקת החשמל אל 2109 דגם M12
יש לנתק את שני כבלי החשמל. (5)

SJHEB699



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1589
Doc: 3690

Hungarian

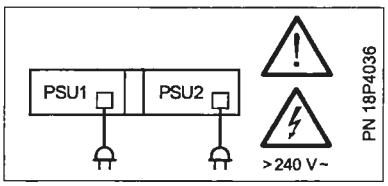
Biztonsági előírások

A biztonsági előírások a könyvben számos helyen megjelennek.

- A *Veszély* felirat figyelmeztet azokra a helyzetekre vagy eljárásokra, amelyek halált vagy súlyos testi sérülést eredményezhetnek.
- A *VIGYÁZAT* felirat olyan veszélyekre hívja fel a figyelmet,amelyek közepes vagy könnyebb személyi sérülést okozhatnak.
- A *Figyelem* felirat figyelmeztet azokra a helyzetekre vagy eljárásokra, amelyek károsíthatják a gépeket, berendezéseket vagy programokat.

Az egyes előírások végén található, zárójeben lévő hivatkozási számok, például (1), segítségével megtalálhatja a kivánt fordítást.

FIGYELEM:
Az egység két tápkábellel rendelkezik. Az áramtalanításhoz húzza ki mindké tápkábelt. (1)



Az Egyesült Államokban csak olyan GBIC egységeket vagy száloptikás termékeket használjon, amelyek megfelelnek az FDA sugárzási szabványok 21CFR J alfejezetének. Nemzetközileg csak olyan GBIC egységeket vagy száloptikás termékeket használjon, amelyek megfelelnek az IEC 825-1-es szabványának. A szabványoknak nem megfelelő optikai termékek fénye károsíthatja a szemet. (2)

SJ000338

VIGYÁZAT

A lítium akkumulátor tüzet, robbanást vagy súlyos égést okozhat. Ne töltse újra, ne szerelje szét, ne hevítse 100°C fölé, ne forrasszon közvetlenül a telepre, ne égesse el és ne tegye ki víz hatásának a telep tartalmát. Tartsa távol a gyermekektől. Kizárólag a rendszerhez megadott termékszámú t egységgel cserélje. Más akkumulátor használata tűz vagy robbanásveszélyes. Az akkumulátorcsatlakozó polarizált; a polaritást ne cserélje föl. A használt akkumulátort a helyi előírásoknak megfelelően kell kezelni. (3)

SJHUN347

FIGYELMEZTETÉS:
Az akkumulátor helytelen cseréje robbanásveszélyt okoz. A használt akkumulátorokat a gyártó utasításai szerint kell kezelni. Keresse meg az IBM-et, ha az óra elkezd késni! (4)

FIGYELMEZTETÉS:
Mindkét tápkábelt húzza ki, ha meg akarja szüntetni a 2109 M12 egység tápellátását! (5)

SJHUN699

Italian

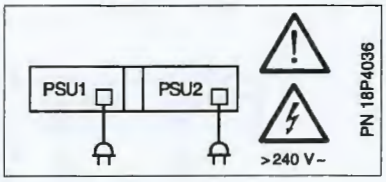
Informazioni sulla sicurezza

Le informazioni sulla sicurezza vengono stampate con questo manuale in modo completo.

- Una nota di Pericolo segnala condizioni o procedure che possono risultare estremamente dannose o pericolose per la persona.
- Una nota di Attenzione segnala condizioni o procedure che possono causare danni o lesioni personali che non sono né letali né estremamente pericolosi.
- Una nota di Avvertenza segnala condizioni o procedure che possono causare danni alle macchine, all'apparecchiatura o ai programmi.

Utilizzare i numeri di riferimento in parentesi, ad esempio (1), alla fine di ciascuna nota per ottenere la traduzione desiderata corrispondente.

AVVERTENZA:
E' possibile che questa unità sia dotata di due cavi di linea. Per rimuovere l'alimentazione, scollegare entrambi i cavi di linea. (1)



ATTENZIONE:
Negli Stati Uniti utilizzare solo unità GBIC o prodotti in fibra ottica, compatibili agli standard di radiazione FDA, 21 CFR Subchapter J. A livello internazionale, utilizzare solo unità GBIC o prodotti in fibre ottiche compatibili con lo standard IEC 825-1. I prodotti ottici che non sono compatibili con questi standard potrebbero produrre luminosità pericolosa agli occhi. **(2)**

SJ000338

ATTENZIONE:
Una batteria a litio può causare incendio, esplosione o gravi ustioni. Non ricaricare, disassemblare, riscaldare al di sopra dei 100°C, saldare direttamente sulla cella, incenerire o esporre il contenuto delle celle in prossimità di acqua. Tenere lontano dalla portata dei bambini. Sostituire solo il numero parte specificato per il sistema. L'utilizzo di un'altra batteria potrebbe provocare un rischio di incendio o di esplosione. Il connettore della batteria è polarizzato; non tentare di invertire la polarità. Smaltire la batteria in base alle norme locali vigenti. (3)

SJITA347

ATTENZIONE:
Se la batteria non viene posizionata correttamente vi è pericolo di esplosione. Tutte le batterie usate devono essere smaltite secondo le istruzioni del produttore. Contattare l' IBM se l'orologio non è preciso. (4)

ATTENZIONE:
Per arrestare l'alimentazione del Modello M12 2109, disconnettere entrambi i cavi di alimentazione . (5)

SJITA699

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1590
Doc: 3690

Japanese

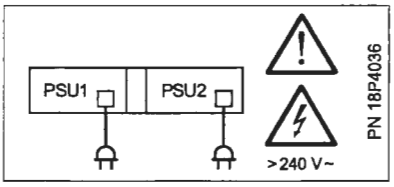
安全上の注意

安全上の注意は、本書全体にわたって印刷されています。

- 「危険」の見出しの付いている項目は、生命の危険を及ぼす、あるいは重傷を負わせる可能性のある状態または手順についての警告です。
- 「注意」の見出しの付いている注意事項は、生命の危険を及ぼすもの、あるいは非常に危険なものではないが、身体を傷つける可能性のある状態または手順についての警告です。
- 「注意」の見出しの付いている注意事項は、マシン、機器、またはプログラムに損傷を与える可能性のある状態または手順についての警告です。

それぞれの注意事項の終わりにある括弧の付いた数字、たとえば (1) を使って、必要な翻訳を選んでください。

注意
この装置には 2 つの回線コードを付けることができます。電源を完全に遮断するには、回線コードを 2 本とも外してください。(1)



注意
米国では、FDA 放射特性規定 21 CFR 副章 J に準拠する GBIC 装置または光ファイバー製品だけを使用してください。米国以外では、IEC 規定 825-1 に準拠する GBIC 装置または光ファイバー製品だけを使用してください。これらの規定に準拠していない光学式製品を使用すると、目に有害な光が出ることがあります。

(2)

SJ000338

注意
リチウム・バッテリーは火事を起こしたり、爆発したり、ひどく燃えたりすることがあります。充電したり、分解したり、100° C (212° F) 以上に熱したり、セルに直接はんだ付けしたり、焼却したり、セルの内容を水に露出したりしないでください。子供の手の届くところに置かないでください。交換する場合はご使用のシステムで決められている部品番号のものだけを使ってください。別のバッテリーを使うと火事や爆発を起こすおそれがあります。バッテリー・コネクターは分極されています。極性を逆にしないでください。バッテリーは地方自治体の規定に従って処分してください。(3)

SJJPN347

注意:
バッテリーは、正しくない方法で交換すると爆発する恐れがあります。
すべての使用済みバッテリーは、製造元の指示に従って廃棄してください。
もしリアルタイム・クロックが遅れるようになりましたら、IBM にご連絡ください。(4)

注意:
2109 モデル M12 への電力を除去するために、電源ケーブルを両方とも切り離してください。(5)

SJJPN699

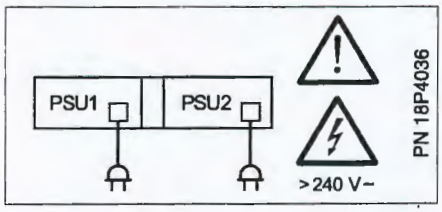
안전 정보

이 책에는 다음의 안전 정보가 표시됩니다.

- 위험사항은 사망이나 중상을 일으킬 수 있는 상태 또는 절차에 대해 경고합니다.
- 주의사항은 치명적이거나 아주 위험하지는 않은 신체적인 상해를 일으킬 수 있는 상태 또는 절차에 대해 경고합니다.
- 유의사항은 기계, 장비 또는 프로그램을 손상시킬 수 있는 상태 또는 절차에 대해 경고합니다.

각 사항의 끝에 있는 괄호 안의 참조 번호(예를 들면, (1))를 참고하십시오.

주의:
이 장치에 두 개의 전원 코드가 있을 수 있습니다. 모든 전원을 제거하려면, 두 개의 전원 코드의 연결을 모두 빼십시오. (1)



경고:
미국에서는 미식약청(FDA) 방사 성능 표준, 21 CFR 부칙 J를 준수하는 GBIC 장치나 광제품만을 사용할 수 있습니다. 국제적으로는 국제 전기 기술 위원회(IEC) 표준 825-1을 준수하는 GBIC 장치나 광제품만을 사용할 수 있습니다. 이 표준을 준수하지 않는 광제품은 눈에 해로운 광선을 방사할 수도 있습니다. (2)

SJ000338

경고:
리튬 배터리는 화재, 폭발 또는 중화상의 원인을 일으킬 수 있습니다. 리튬 배터리는 재충전하거나 해체해서는 안되며, 섭씨 100도(화씨 212도) 이상의 열에 노출시켜서는 안됩니다. 또한 셀에 직접 납땜하거나 이를 소각하지 마시고 셀 내용물이 물에 닿지 않게 하십시오. 어린이의 손에 닿지 않게 하십시오. 시스템에 지정된 부품 번호로만 교체하십시오. 다른 배터리를 사용하면 화재나 폭발을 일으킬 수도 있습니다. 배터리 커넥터는 극성을 띠고 있으므로 양극을 바꾸어 사용하지 마십시오. 지역 규정에 따라 배터리를 폐기하십시오. (3)

SJKOR347

주의:
배터리를 잘못 대체한 경우 폭발의 위험이 있습니다. 사용된 모든 배터리는 제조업체의 지시사항에 따라 폐기해야 합니다. 실시간 시계가 늦기 시작하면 IBM에 문의하십시오. (4)

주의:
2109 Model M12의 전원을 제거하려면 양쪽 전원 케이블의 연결을 모두 끊으십시오. (5)

SJKOR699

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1591
3690
Doc:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1592
Doc: 3690

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1593
Doc 3690

Macedonian

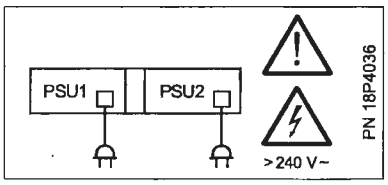
Забелешки за сигурност

Забелешките за сигурност се наоѓаат на крајот од оваа книга.

- Забелешките за опасност се однесуваат на условите и процедурите кои можат да предизвикаат повреди на пресоналот кои можат да предизвикаат смрт.
- Забелешките за внимание се однесуваат на условите и процедурите кои можат да предизвикаат повреди на пресоналот кои не се смртоносни или екстремно опасни.
- Забелешките за предупредување се однесуваат на условите и процедурите кои можат да предизвикаат штета на машините, опремата, или програмите.

Користете ги броевите во загради за референцирање, на пр.(1), на крајот на секоја забелешка за да се референцирате на саканиот превод.

ВНИМАНИЕ:
Оваа единица може да има два кабли за напојување. За да го исклучите напојувањето целосно исклучете ги двата кабли. (1)



ВНИМАНИЕ:
Во САД користете само GBIC уреди или Фибер-Оптички продукти кои ги исполнуваат FDA стандардите за радијација, 21 CFR подзагалавие J. Интернационално користете само GBIC уреди или Фибер-Оптички продукти кои го исполнуваат IEC стандардот 825-1. Оптичките продукти кои не ги исполнуваат овие стандарди може да предизвикаат светлина која е опасна за очите. (2)

SJ000338

ВНИМАНИЕ:
Литиумската батерија може да предизвика пожар, експлозија, или сериозни изгореници. Не ја полнете повторно, не ја расклопувајте, не ја загревајте над 100°C (212°F), не ја лемете директно на ќелијата, не ја палете, или не ја изложувајте содржината на ќелијата на вода. Чувајте ја подалеку од деца. Заменете ја само со дел специфициран за Вашиот систем. Користење на друга батерија претставува ризик од пожар или експлозија. Конекторот на батеријата е поларизиран, не се обидувајте да го смените поларитетот. Отстранувањето на искористените батерии се врши според локалните регулативи. (3)

SJMAC347

ВНИМАНИЕ:
Постои опасност од експлозија ако батеријата непрописно се заменува. Сите искористени батерии мора да се уништат според препораките на нивниот производувач. Контактирајте го IBM ако real time clock чипот губи информација за времето. (4)

ВНИМАНИЕ:
при исклучувањето на 2109 модел M12, исклучете ги двата мрежни (струјни) кабли. (5)

SJMKD699

Portuguese

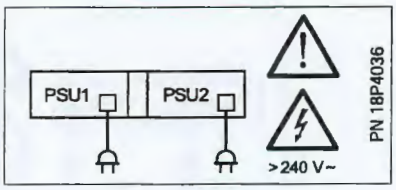
Avisos de Segurança

Os avisos de segurança encontram-se impressos ao longo deste manual.

- Um aviso de *Perigo* informa o utilizador de que há condições ou procedimentos que podem resultar em morte ou em graves danos pessoais.
- Um aviso de *Cuidado* informa o utilizador da existência de condições ou procedimentos que podem resultar em danos pessoais que não são mortais nem potencialmente perigosos.
- Um aviso de *Atenção* informa o utilizador da existência de condições ou procedimentos que podem causar danos a máquinas, equipamento, ou programas.

Recorra aos números de referência entre parêntesis (1) no final de cada aviso para saber qual a tradução pretendida.

CUIDADO:
Esta unidade poderá dispor de dois cabos eléctricos. Para cortar a alimentação desligue ambos os cabos. (1)



CUIDADO:
Nos Estados Unidos utilize apenas unidades GBIC ou produtos de Fibra-Óptica que estejam em conformidade com as normas de rendimento de radiação da FDA, 21 CFR Subcapítulo J. Internacionalmente utilize apenas unidades GBIC ou produtos de Fibra-Óptica que estejam em conformidade com a norma 825-1 da IEC. Produtos Ópticos que não estejam em conformidade com estas normas podem produzir luz que é perigosa para a vista. (2)

SJ000338

CUIDADO:
Uma pilha de lítio pode provocar fogo, explosão ou uma queimadura grave. Não recarregar, desmontar, aquecer acima dos 100°C (212°F), soldar directamente na pilha, incinerar, ou expor o conteúdo da pilha à água. Manter afastado das crianças. Substituir apenas pelo part number especificado para o sistema. A utilização de outra bateria pode apresentar um risco de fogo ou de explosão. O conector da pilha está polarizado; não tente inverter a polaridade. Deite a bateria fora de acordo com os regulamentos locais. (3)

SJPOR347

CUIDADO:
Perigo de explosão se a pilha for incorrectamente substituída.
Para deitar fora pilhas usadas, siga as instruções do fabricante.
Contacte a IBM se o relógio de tempo real começar a atrasar. (4)

CUIDADO:
Para desligar a alimentação do 2109 Modelo M12, desligue ambos os cabos de alimentação. (5)

SJPTG699

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1594
Doc: 3690

Russian

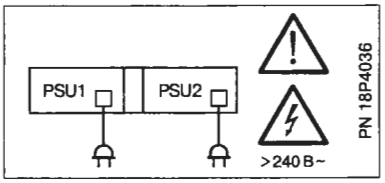
Замечания по технике безопасности

В этой книге встречаются замечания по технике безопасности.

- Замечания под заголовком *Опасно* предупреждают об условиях или операциях, которые, могут повлечь за собой смертные случаи или серьезные травмы.
- Замечания под заголовком *Осторожно* предупреждают об условиях или операциях, которые могут явиться причиной травм, но не приведут ни к смертным случаям, ни к особо серьезным поражениям.
- Замечания под заголовком *Внимание* предупреждают об условиях или операциях, которые могут привести к порче компьютеров, оборудования или программ.

Чтобы найти перевод нужного замечания, смотрите номер, указанный в скобках в конце этого замечания, например, (1).

ОСТОРОЖНО:
У этого блока может быть два шнура питания. Чтобы полностью отключить питание, отсоедините оба шнура. (1)



ОСТОРОЖНО:
В США следует применять только блоки GBIC и оптоволоконные устройства, отвечающие требованиям стандартов FDA по уровню излучения, CFR 21, подраздел J.
В других странах следует применять только блоки GBIC и оптоволоконные устройства, отвечающие требованиям стандарта IEC 825-1. Оптические устройства, не отвечающие этим стандартам, могут излучать свет, опасный для глаз. (2)

SJ000338

ОСТОРОЖНО:
Неосторожное обращение с литиевой батареей может привести к пожару, взрыву или серьезным ожогам. Не заряжайте и не разбирайте батарею, не нагревайте ее до температуры выше 100°C (212°F), не паяйте и не сжигайте ее, не допускайте контакта содержимого батареи с водой. Берегите от детей. Заменяйте только на батарею с кодом, соответствующим вашей системе. Применение другой батареи может привести к взрыву или пожару. При подключении батареи обязательно соблюдайте полярность. Утилизируйте батарею в соответствии с местным законодательством. (3)

SJRUS347

ОСТОРОЖНО:
При неправильной замене батарейки возможен взрыв. Все использованные батарейки следует утилизировать в соответствии с инструкциями изготовителя. Если часы реального времени начнут отставать, обращайтесь в IBM. (4)

ОСТОРОЖНО:
Чтобы отключить питание 2109 Model M12, отсоедините оба шнура питания. (5)

SJRUS699

Slovak

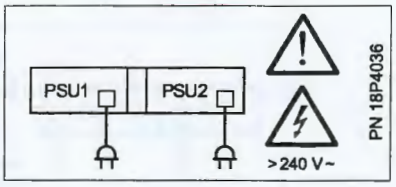
Bezpečnostné oznamy

Bezpečnostné oznamy sa nachádzajú všade v tejto knihe.

- Oznam o nebezpečenstve vás varuje pred stavmi a postupmi, ktoré môžu mať za následok smrť alebo vážne osobné zranenie.
- Výstraha vás varuje pred stavmi a postupmi, ktoré môžu spôsobiť osobné zranenie, ktoré nie je ani smrteľné ani extrémne nebezpečné.
- Upozornenie vás varuje pred stavmi a postupmi, ktoré môžu spôsobiť poškodenie strojov, zariadenia alebo programov.

Požadovaný preklad nájdete podľa referenčného čísla v zátvorkách, napríklad (1), ktoré sa nachádza na konci každého oznamu.

VÝSTRAHA:
Táto jednotka môže mať dva napájacie káble. Aby ste odstránili všetko napájanie, odpojte obidva káble. (1)



VÝSTRAHA:
V Spojených štátoch používajte len jednotky GBIC alebo optické produkty, ktoré vyhovujú radiačným štandardom FDA, 21 CFR podkapitola J.
V ostatných krajinách používajte len jednotky GBIC alebo optické produkty, ktoré vyhovujú IEC štandardu 825-1. Optické produkty, ktoré nevyhovujú týmto štandardom, môžu produkovať žiarenie, ktoré je nebezpečné pre oči. (2)

SJ000338

VÝSTRAHA:
Lítiová batéria môže spôsobiť požiar, výbuch alebo silné popálenie. Nedobíjajte, nerozoberajte, nezohrievajte nad 100°C, nespájkujte priamo články, nespaľujte ani nesypte obsah článkov do vody. Držte mimo dosah detí. Nahradzujte ju len batériou s číslom dielu, ktoré je uvedené pre váš systém. Použitie inej batérie môže znamenať riziko požiaru alebo výbuchu. Batéria je polarizovaná; nepokúšajte sa vymeniť polaritu. Batérie sa zbavte podľa miestnych predpisov. (3)

SJSLK347

VÝSTRAHA:
Ak je batéria nesprávne vymenená, existuje nebezpečenstvo výbuchu. Všetky použité batérie musia byť znehodnotené v súlade s pokynmi výrobcu.
Ak hodiny reálneho času začínajú meškať, obráťte sa na IBM. (4)

VÝSTRAHA:
Ak chcete odstrániť napájanie pre 2109 Model M12, odpojte obidva napájacie káble. (5)

SJSKY699

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1595
3690
Doc:

Slovenian

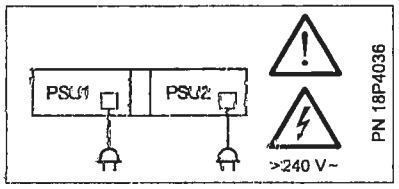
Opombe o varnosti

Opombe o varnosti so natisnjene na več mestih v tej knjigi.

- Opomba o nevarnosti vas opozarja na stanja ali postopke, ki lahko povzročijo smrt ali resne osebne poškodbe.
- Opomba o previdnosti vas opozarja na stanja ali postopke, ki lahko povzročijo osebne poškodbe, ki pa niso smrtne ali zelo hude.
- Varnostno opozorilo vas opozarja na stanja ali postopke, ki lahko povzročijo poškodbe na strojih, opremi ali programski opremi.

Referenčne številke v oklepajih, na primer (1), na koncu vsakega opozorila uporabite za uskladitev z želenim prevodom.

OPOZORILO:
Ta enota ima lahko dva priključka za omrežno napetost. Če želite v celoti odstraniti napajanje, izključite oba napajalna kabla. (1)



OPOZORILO:
V ZDA uporabljajte le enote GBIC ali izdelke z optičnimi vodniki, ki se skladajo s standardi FDA, 21 CFR podpoglavje J. Drugje po svetu uporabljajte le enote GBIC ali izdelke z optičnimi vodniki, ki se skladajo s standardom IEC 825-1. Optični izdelki, ki se ne skladajo s temi standardi, lahko oddajajo svetlobo, ki je škodljiva očem. (2)

SJ000338

OPOZORILO:
Litijeva baterija lahko povzroči požar, eksplozijo ali resne opekline. Zato je znova ne polnite, razstavite, segrevajte na temperature nad 100°C (212°F), prispajkajte neposredno na celico, sežgite ali izpostavljajte vsebine vodi. Hranite jo tako, da do nje ne bodo imeli dostopa otroci. Zamenjajte jo le s sestavnim delom, katerega številka je podana za vaš sistem. Uporaba druge baterije lahko povzroči požar ali eksplozijo. Spojnik baterije je polariziran; ne poskušajte zamenjati polaritete. Baterijo odvrzite v skladu z lokalnimi predpisi. (3)

SJSLV347

OPOZORILO:
Če baterije ne vstavite na pravilno mesto, lahko pride do eksplozije. Vse izrabljene baterije morate usmetiščiti v skladu z navodili proizvajalca. Če ura dejanskega časa začne zaostajati, se obrnite na IBM. (4)

OPOZORILO:
Če želite odstraniti napajanje za model M12 računalnika 2109, izključite oba napajalna kabla. (5)

SJSLV699

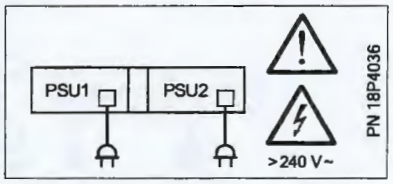
Avisos de seguridad

Los avisos de seguridad están impresos a lo largo de este manual.

- Un aviso de *Peligro* le avisa sobre condiciones o procedimientos que pueden causar la muerte o provocar daños personales graves.
- Un aviso de *Precaución* le avisa sobre condiciones o procedimientos que pueden causar daños personales que no provocan la muerte ni son muy peligrosos.
- Un aviso de *Atención* avisa sobre condiciones o procedimientos que pueden causar daños en máquinas, equipo o programas.

Utilice los nombres de referencia en paréntesis como, por ejemplo, (1) que se encuentran al final de cada aviso para saber cuál es la traducción deseada.

PRECAUCIÓN:
Esta unidad puede tener dos cables eléctricos. Para eliminar toda la alimentación, desconecte los dos cables. (1)



PRECAUCI N:
En los Estados Unidos utilice solamente unidades GBIC o productos de Fibra óptica que cumplan con los estándares de rendimiento de radiación de FDA, 21 CFR Subcapítulo J. A nivel internacional, utilice solamente unidades GBIC o productos de Fibra óptica que cumplan con el estándar 825-1 de IEC. Los productos ópticos que no cumplan dichos estándares pueden emitir luz perjudicial para la vista. (2)

SJ000338

PRECAUCIÓN:
Una batería de litio puede provocar incendios, explosiones o quemaduras graves. No se debe recargar, desmontar, calentar por encima de los 100 °C (212 °F), soldar directamente a la célula, incinerar ni exponer a humedades. Manténgase fuera del alcance de los niños. Sustituya solamente con el número de pieza especificado para su sistema. El utilizar otra batería puede implicar peligro de incendio o explosión. El conector de la batería está polarizado; no intente invertir la polaridad. Deseche la batería de acuerdo a las regulaciones locales. (3)

SJSPA347

PRECAUCIÓN:

Existe riesgo de explosión si la batería se sustituye de forma incorrecta. Todas las baterías usadas deben desecharse de acuerdo con las instrucciones del fabricante. Póngase en contacto con IBM si el reloj de tiempo real comienza a atrasarse. (4)

PRECAUCIÓN:
Para desconectar el conmutador 2109 Modelo M12 de la corriente eléctrica, desenchufe los dos cables de alimentación. (5)

SJSPA699

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1596
Doc: 3690

Swedish

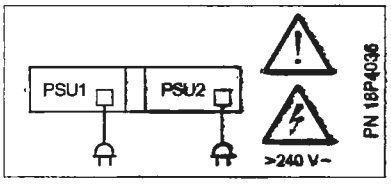
Säkerhetsinformation

Den här boken innehåller säkerhetsinformation.

- Meddelanden som föregås av ordet Fara varnar för tillstånd eller procedurer som kan orsaka död eller allvarlig personskada.
- Meddelanden som föregås av ordet Varning varnar för tillstånd eller procedurer som kan orsaka personskada som är vare sig dödlig eller extremt hälsovådlig.
- Meddelanden som föregås av ordet Obs varnar för tillstånd eller procedurer som kan orsaka skada på datorer, utrustning eller program.

Använd referensnumren inom parentes i slutet av varje meddelande, t ex (1), för en viss översättning.

VARNING:
Den här enheten kan ha två nätkablar. Koppla ur båda nätkablarna så att all ström bryts. (1)



VARNING:
I USA ska endast GBIC-enheter eller fiberoptiska produkter som uppfyller FDA-standarder för strålning, 21 CFR avsnitt J, användas. Internationellt ska endast GBIC-enheter eller fiberoptiska enheter som uppfyller IEC-standard 825-1 användas. Optiska produkter som inte uppfyller standarderna kan utstråla ljus som är skadligt för ögonen. (2)

SJ000338

VARNING:

Litiumbatterier kan orsaka brand, explosioner eller allvarliga brännskador. Batteriet får inte laddas om, hettas upp till mer än 100 grader celsius eller tas isär. Battericellen får inte lödas direkt på eller brännas, och dess innehåll får inte utsättas för vatten. Låt inte barn leka med batterierna. Ersätt bara med batterier med artikelnumret som gäller för det system du använder. Det kan innebära risk för eldsvåda eller explosion att använda ett batteri av annan typ. Försök aldrig kasta om batteriets poler. Följ lokala miljöföreskrifter när du slänger batteriet. (3)

SJSWE347

VARNING:
Det finns fara för explosion om batteriet byts ut på ett felaktigt sätt. Släng det använda batteriet i enlighet med tillverkarens anvisningar.
Kontakta IBM om klockan börjar gå långsammare. (4)

VARNING:
Bryt strömmen till 2109 modell M12 genom att koppla ur båda strömkablarna. (5)

SJSVE699

Notices

This information was developed for products and services offered in the U. S. A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, N.Y. 10504–1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2002, 2003

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1597
51
Doc: 3690

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM
TotalStorage

Other company, product, or service names may be trademarks or service marks of others.

Electronic emission statements

This section gives the electronic emission notices or statements for the United States and other countries.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada compliance statement

Avis de conformite a la reglementation d'Industrie Canada: Cet appareil numerique de la classe A est conform a la norme NMB-003 du Canada.

Chinese Class A compliance statement

Attention: This is a Class A statement. In a domestic environment, this product might cause radio interference in which case the user might be required to take adequate measures.

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

European Community compliance statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product is in conformity with the EU council directive 73/23/EEC on the approximation of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits. This conformity is based on compliance with the following harmonized standard: EN60950.

This product has been tested and found to comply with the limits for class A Information Technology Equipment according to European Standard EN 55022. The limits for class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Where shielded or special cables (for example, cables fitted with ferrites) are used in the test to make the product comply with the limits:

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorized dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

Germany compliance statement

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische

Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG das

EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuellt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

2005 - CN -
CORREIOS
1598
Fls. No.
3690
Doc:

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:_|t[1]|

"Geraete duerfen an Orten, fuer die sie nicht ausreichend entstoert sind, nur mit besonderer Genehmigung des Bundesministeriums fuer Post und Telekommunikation oder des Bundesamtes fuer Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Stoerungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs.4)

Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden

Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Nach der EN 55022:

"Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstoerungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzufuehren und dafuer aufzukommen."

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen, sind die Geraete wie in den Handbuechern angegeben zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Government Ministry of Communication (MOC) statement

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find that this is not suitable for your use, you may exchange it for one with a non-business use.

Taiwan class A compliance statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用
時，可能會造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。 VS07171L

Glossary

This glossary provides definitions for the Fibre Channel and switch terminology used for the IBM 2109 Model M12. This glossary also provides definitions for the Fibre Channel and switch terminology used for the IBM TotalStorage SAN Cabinet 2109 Model C36.

This glossary defines technical terms and abbreviations used in this document. If you do not find the term you are looking for, see the *IBM Glossary of Computing Terms* located at www.ibm.com/networking/nsg/nsgmain.htm

This glossary also includes terms and definitions from:

- *Information Technology Vocabulary* by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- *IBM Glossary of Computing Terms.* New York: McGraw-Hill, 1994.

The following cross-reference conventions are used in this glossary:

See Refers you to (a) a term that is the expanded form of an abbreviation or acronym, or (b) a synonym or more preferred term.

See also Refers you to a related term.

8b/10b encoding. An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports

16-port card. The Fibre Channel port card provided with the 2109 Model M12. Contains 16 ports and the corresponding light-emitting diodes (LEDs). See also *port card.*

access control list (ACL). Enables an organization to bind a specific worldwide name (WWN) to a specific switch port or set of ports, preventing a port in another physical location from assuming the identity of a real WWN. Can also refer to a list of the read/write access of a particular community string. See also *device connection controls.*

account level switches. Switches that have four login accounts into the operating system (in descending order): root, factory, admin, and user. See also *admin account.*

ACL. See *access control list.*

address identifier. A 24-bit or 8-bit value used to identify the source or destination of a frame.

admin account. A login account intended for use by the customer to control switch operation. See also *account level switches.*

alias. An alternate name for an element or group of elements in the fabric. Aliases can be used to simplify the entry of port numbers and worldwide names (WWNs) when creating zones.

alias address identifier. An address identifier recognized by a port in addition to its standard identifier. An alias address identifier can be shared by multiple ports.

alias AL_PA. An arbitrated loop physical address (AL_PA) value recognized by a loop port (L_port) in addition to the AL_PA assigned to the port. See also *arbitrated loop physical address.*

alias server. A fabric software facility that supports multicast group management.

AL_PA. See *arbitrated loop physical address.*

American National Standards Institute (ANSI). The governing body for Fibre Channel standards in the U.S.A.

ANSI. See *American National Standards Institute.*

API. See *application programming interface.*

application programming interface (API). A defined protocol that allows applications to interface with a set of services.

application-specific integrated circuit (ASCI). In computer chip design, an integrated circuit created by first mounting an array of unconnected logic gates on a substrate and later connecting these gates in a particular configuration for a specific application. This design approach allows chips for a variety of applications to be made from the same generic gate array, thereby reducing production costs.

ARB. See *arbitrate primitive signal.*

© Copyright IBM Corp. 2002, 2003

RCS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1599
55
3690
Doc:

arbitrate primitive signal (ARB). A primitive signal that is transmitted as the fill word by a loop port (L_port) to indicate that the L_port is arbitrating to access to the loop. Applies only to the arbitrated loop topology.

arbitrated loop. A shared 100 MBps Fibre Channel transport structured as a loop and supporting up to 126 devices and one fabric attachment. A port must successfully arbitrate before a circuit can be established.

arbitrated loop physical address (AL_PA). An 8-bit value used to uniquely identify an individual port within a loop. A loop can have one or multiple AL_PAs.

arbitration wait timeout value (AW_TOV). The minimum time an arbitrating loop port (L_port) waits for a response before beginning loop initialization.

area number. A number that is assigned to each potential port location in the switch. Used to distinguish ports that have the same port number but are on different port cards.

ASIC. See *application-specific integrated circuit.*

asynchronous transfer mode (ATM). A broadband technology for transmitting data over local area networks (LANs) or wide area networks (WANs), based on relaying cells of fixed size. Provides any-to-any connectivity, and nodes can transmit simultaneously.

ATM. See *asynchronous transfer mode.*

auto-negotiate speed. Process that allows two devices at either end of a link segment to negotiate common features, speed (for example, 1 Gbps or 2 Gbps) and functions.

autoranging. A power supply that accommodates different input voltages and line frequencies.

autosense. Process during which a network device automatically senses the speed of another device.

AW_TOV. See *arbitration wait timeout value.*

backup FCS switch. The switch or switches assigned as backup in case the primary fabric configuration server (FCS) switch fails. See also *fabric configuration server switch* and *primary FCS switch.*

bandwidth. (1) The total transmission capacity of a cable, link, or system. Usually measured in bits per second (bps). (2) The range of transmission frequencies available to a network. See also *throughput.*

basic input/output system (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

BB_credit. See *buffer-to-buffer credit.*

beacon. When all the port light-emitting diodes (LEDs) on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by Telnet command or through Web Tools.

beginning running disparity. The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. See also *disparity.*

BER. See *bit error rate.*

BIOS. See *basic input/output system.*

BISR. Built-in self-repair.

bit error rate (BER). The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted. See also *error.*

blade. One component in a system that is designed to accept some number of components (blades). Blades could be individual servers that plug into a multiprocessing system or individual port cards that add connectivity to a switch. A blade is typically a hot swappable hardware device. See *16-port card.*

blind-mate connector. A two-way connector used in some switches to provide a connection between the system board and the power supply.

block. As applies to fibre channel, upper-level application data that is transferred in a single sequence.

bloom. Application-specific integrated circuit (ASIC) technology that the 2109 Model M12 is based on.

boot flash. Flash memory that stores the boot code and boot parameters. The processor runs its first instructions from boot flash. Data is cached in random access memory (RAM).

boot monitor. Code used to initialize the control processor (CP) environment after powering on. Identifies the amount of memory available and how to access it, and retrieves information about system buses.

British thermal unit (BTU). A measurement of heat produced in one hour.

broadcast. The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *multicast* and *unicast.*

BTU. See *British thermal unit.*

buffer-to-buffer credit. The number of frames that can be transmitted to a directly-connected recipient or within an arbitrated loop. Determined by the number of receive buffers available. See also *buffer-to-buffer flow control.*

buffer-to-buffer flow control. Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop. See also *buffer-to-buffer credit.*

CAM. Content addressable memory.

cascade. Two or more interconnected Fibre Channel switches that can build large fabrics. Switches can be cascaded up to 239 switches, with a recommended maximum of seven inter-switch links (no path longer than eight switches). See also *fabric* and *inter-switch link.*

central processing unit (CPU). A part of a computer that includes the circuits that control the interpretation and execution of instructions. A CPU in the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

chassis. The metal frame in which the switch and switch components are mounted.

circuit. An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions. See also *link.*

class 1. Service that provides a dedicated connection between two ports (also called connection-oriented service), with notification of delivery or nondelivery.

class 2. Connectionless service between ports with notification of delivery or nondelivery.

class 3. Connectionless service between ports without notification of delivery. Other than notification, the transmission and routing of class 3 frames is the same as class 2 frames.

class F. Connectionless service for inter-switch control traffic. Provides notification of delivery or nondelivery between two expansion ports (E_ports).

class of service. A specified set of delivery characteristics and attributes for frame delivery.

CLI. See *command line interface.*

CMI. Control message interface.

comma. A unique pattern (either 1100000 or 0011111) used in 8b/10b encoding to specify character alignment within a data stream. See also *K28.5.*

command line interface (CLI). Interface that depends entirely on the use of commands, such as through Telnet or simple network management protocol (SNMP), and does not involve a graphical user interface.

community (SNMP). A relationship between a simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

compact flash. Flash memory that stores the run-time operating system and is used like hard disk storage. Not visible within the memory space of the processor. Data is stored in file system format. Also called user flash.

control processor (CP). The central processing unit that provides all control and management functions in a switch.

control processor card (CP card). The central processing unit of the 2109 Model M12, which contains two control processor (CP) card slots to provide redundancy. Provides Ethernet, serial, and modem ports with the corresponding light-emitting diodes (LEDs).

core switch. A switch whose main task is to interconnect other switches. Also referred to as a backbone switch. See also *edge switch.*

CP. See *control processor.*

CP card. See *control processor card.*

CPLD. Complex programmable logic device.

CPU. See *central processing unit.*

CRC. See *cyclic redundancy check.*

credit. When applied to a switch, the maximum number of receive buffers provided by a fabric port (F_port) or fabric loop port (FL_port) to its attached node port (N_port) or node loop port (NL_port), respectively, such that the N_port or NL_port can transmit frames without over-running the F_port or FL_port.

CSA. Canadian Standards Association.

cut-through. A switching technique that allows the route for a frame to be selected as soon as the destination address is received. See also *route.*

cyclic redundancy check (CRC). A check for transmission errors included in every data frame.

data communications equipment (DCE) port. A port that is capable of interfacing between a data terminal equipment (DTE) port and a transmission circuit. DCE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2. See also *data terminal equipment (DTE) port.*

data rate. The rate at which data is transmitted or received from a device. Interactive applications tend to require a high data rate, while batch applications can usually tolerate lower data rates.

CPMI - CORREIOS
Fls. Nº 1600
Doc: 3690

data terminal equipment (DTE) port. A port that is capable of interfacing to a transmission circuit through a connection to a data communications equipment (DCE) port. DTE devices with an RS-232 (or EIA-232) port interface transmit on pin 3, and receive on pin 2 in a 9-pin connector (reversed in 25-pin connectors). See also *data communications equipment (DCE) port*.

DB-9 connector. A 9-pin version of the RS-232C port interface.

DCC. A dc converter.

DCE port. See *data communications equipment (DCE) port*.

DDR. Double data rate. See *data rate*.

defined zone configuration. The complete set of all zone objects that are defined in the fabric. The defined configuration can include multiple zone configurations. See also *enabled zone configuration* and *zone configuration*.

device. Hosts and storage that connect to a switch. Example devices are servers, redundant array of independent disks (RAID) arrays, and tape subsystems.

device connection controls. Enables organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by a worldwide name (WWN) and typically represent host bus adapters (HBAs) (servers). See also *access control lists*.

DID. The 3-byte destination ID of the destination device, in the 0xDomainAreaALPA format.

direct memory access (DMA). The transfer of data between memory and an input/output device without processor intervention.

disparity. The relationship of ones and zeros in an encoded character. *Neutral disparity* means an equal number of each, *positive disparity* means a majority of ones, and *negative disparity* means a majority of zeros.

DLS. See *dynamic load sharing*.

DMA. See *direct memory access*.

DNS. Distributed name server.

domain_ID. Unique identifier for the switch in a fabric. Usually automatically assigned by the switch, but can also be assigned manually. Can be any value between 1- 239.

DRAM. See *dynamic random access memory*.

DTE port. See *data terminal equipment (DTE) port*.

dual fabric. Two identical fabrics that allow redundancy in the event that one fabric fails. Use a dual fabric for mission critical applications.

dual-fabric SAN. A storage area network (SAN) that is composed of two independent fabrics. Synonymous with multi-fabric SAN. The two-fabric architecture makes dual-fabric SANs redundant.

DWDM. Dense wavelength digital multiplexing.

dynamic load sharing (DLS). Dynamic distribution of traffic over available paths. Allows for recomputing of routes when a fabric port or fabric loop port (Fx_port) or expansion port (E_port) changes status.

dynamic random access memory (DRAM). A storage in which the cells require repetitive application of control signals to retain stored data.

edge fabric. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric. See also *resilient core*.

edge switch. A switch whose main task is to connect nodes into the fabric. See also *core switch*.

E_D_TOV. See *error detect timeout value*.

EE_credit. See *end-to-end credit*.

effective zone configuration. The particular zone configuration that is currently in effect. Only one configuration can be in effect at once. The effective configuration is built each time a zone configuration is enabled.

EIA. Electronic Industry Association.

EIA rack. A storage rack that meets the standards set by the Electronics Industry Association (EIA).

electromagnetic compatibility (EMC). The design and test of products to meet legal and corporate specifications dealing with the emissions and susceptibility to frequencies in the radio spectrum. Electromagnetic compatibility is the ability of various electronic equipment to operate properly in the intended electromagnetic environment.

electromagnetic interference (EMI). Waves of electromagnetic radiation, including but not limited to radio frequencies, generated by the flow of electric current.

electrostatic discharge (ESD). The flow of current that results when objects having a static charge come into close enough proximity to discharge.

ELP. Extended link parameters.

ELWL. See *extra long wavelength*.

EMC. See *electromagnetic compatibility*.

EMI. See *electromagnetic interference*.

enabled zone configuration. The currently enabled configuration of zones. Only one configuration can be enabled at a time. See also *defined zone configuration* and *zone configuration*.

end port. A port on an edge switch that connects a device to the fabric.

end-to-end credit (EE_credit). The number of receive buffers allocated by a recipient port to an originating port. Used by class 1 and class 2 services to manage the exchange of frames across the fabric between source and destination. See also *end-to-end flow control* and *buffer-to-buffer credit*.

end-to-end flow control. Governs flow of class 1 and class 2 frames between node ports (N_ports). See also *end-to-end credit*.

E_port. See *expansion port*.

error. As applies to fibre channel, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors). See also *loop failure*.

error detect timeout value (E_D_TOV). The time that the switch waits for an expected response before declaring an error condition. Adjustable in 1 microsecond increments from 2 - 10 seconds.

ESD. See *electrostatic discharge*.

exchange. The highest level Fibre Channel mechanism used for communication between node ports (N_ports). Composed of one or more related sequences, and can work in either one or both directions.

expansion port (E_port). A port is designated an expansion port (E_port) when it is used as an inter-switch expansion port to connect to the E_port of another switch, to build a larger switch fabric.

Extended Fabrics. A feature that runs on Fabric operating system (OS) and allows creation of a Fibre Channel fabric interconnected over distances of up to 100 km (62.14 mi).

extra long wavelength (ELWL). Laser light with a periodic length greater than 1300 nm (for example, 1420 or 1550). ELWL lasers are used to transmit Fibre Channel data over distances greater than 10 km. Also known as XLWL.

fabric. A network that uses high-speed fibre connections to connect switches, hosts, and devices. A fabric is an active, intelligent, nonshared interconnect scheme for nodes.

Fabric Access. Allows the application to control the fabric directly for functions such as discovery, access (zoning) management, performance, and switch control. Consists of a host-based library that interfaces the application to switches in the fabric over an out-of-band TCP/IP connection or in-band using an IP-capable host bus adapter (HBA).

Fabric Assist. A feature that enables private and public hosts to access public targets anywhere on the fabric, provided they are in the same Fabric Assist zone.

fabric configuration server (FCS) switch. One or more designated switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by worldwide name (WWN), and the list of designated switches is communicated fabric-wide. See also *backup FCS switch*, *primary FCS switch*.

fabric login (FLOGI). The process by which a device gains access to the fabric.

fabric loop port (FL_port). A fabric port that is loop capable. Used to connect node loop ports (NL_ports) to the switch in a loop configuration.

Fabric Manager. A feature that allows the storage area network (SAN) manager to monitor key fabric and switch elements, making it easy to quickly identify and escalate potential problems. It monitors each element for out-of-boundary values or counters and provides notification when defined boundaries are exceeded. The SAN manager can configure which elements, such as error, status, and performance counters, are monitored within a switch.

fabric mode. One of the modes for a loop port (L_port). An L_port is in fabric mode when it is connected to a port that is not loop capable and is using fabric protocol. See also *loop port* and *loop mode*.

fabric name. The unique identifier assigned to a fabric and communicated during login and port discovery.

Fabric OS. An operating system made up of two software components: the firmware that initializes and manages the switch hardware, and diagnostics.

fabric port (F_port). A port that is able to transmit under fabric protocol and interface over links. Can be used to connect a node port (N_port) to a switch. See also *fabric loop port* and *Fx_port*.

Fabric Watch. A feature that runs on Fabric operating system (OS) and allows monitoring and configuration of fabric and switch elements.

failover. The act that causes control to pass from one redundant unit to another.

FAN. Fabric address notification.

FC. See *fibre channel*.

FCA. See *Fibre Channel arbitrated loop*.

FC-AL. See *Fibre Channel arbitrated loop*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1601
Doc. 3690

FC-AL-3. The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FCC. Federal Communications Commission.

FC-FLA. The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCMGMT. Fibre Alliance Fibre Channel Management.

FCP. See *Fibre Channel protocol.*

FC-PDLA. The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FC-PH-1,2,3. The Fibre Channel Physical and Signaling Interface standards defined by ANSI.

FC-PI. The Fibre Channel Physical Interface standard defined by ANSI.

FCS switch. See *fabric configuration server switch.*

FC-SW-2. The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches in order to create a multiswitch Fibre Channel fabric.

Fibre Channel (FC). A technology for transmitting data between computer devices at a data rate of up to 4 Gbps. It is especially suited for attaching computer servers to shared storage devices and for interconnecting storage controllers and drives.

Fibre Channel arbitrated loop (FC-AL). A standard defined on top of the FC-PH standard. It defines the arbitration on a loop where several FC nodes share a common medium.

Fibre Channel protocol (FCP). The protocol for transmitting commands, data, and status using Fibre Channel FC-FS exchanges and information units. Fibre channel is a high-speed serial architecture that allows either optical or electrical connections at data rates from 265 Mbps up to 4-Gbps.

Fibre Channel service (FS). A service that is defined by Fibre Channel standards and exists at a well-known address. For example, the Simple Name Server is a Fibre Channel service. See also *Fibre Channel service protocol.*

Fibre Channel service protocol (FSP). The common protocol for all fabric services, transparent to the fabric type or topology. See also *Fibre Channel service.*

Fibre Channel shortest path first (FSPF). A routing protocol used by Fibre Channel switches.

Fibre Channel transport. A protocol service that supports communication between Fibre Channel service providers. See also *Fibre Channel service protocol.*

field replaceable unit (FRU). An assembly that is replaced in its entirety when any one of its components fails. In some cases, a field replaceable unit can contain other field replaceable units.

File Transfer protocol (FTP). In Transmission Control protocol/Internet protocol (TCP/IP), an application protocol used for transferring files to and from host computers.

fill word. An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the Fibre Channel link active.

firmware. The basic operating system provided with the hardware.

FLA. Fabric loop attach.

flash partition. Two redundant usable areas, called *partitions* into which firmware can be downloaded in the 2109 Model M12.

FLOGI. See *fabric login.*

FL_port. See *fabric loop port.*

F_port. See *fabric port.*

frame. The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, the data payload, a cyclic redundancy check (CRC), and an end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements, and so on) and data frames.

frame delimiter. A part of an ordered set that marks frame boundaries and describes frame contents. See also *ordered set.*

FRU. See *field replaceable unit.*

FS. See *Fibre Channel service.*

FSP. See *Fibre Channel service protocol.*

FSPF. See *Fibre Channel shortest path first.*

FTP. See *File Transfer protocol.*

full duplex. A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *half duplex.*

Fx_port. A fabric port that can operate as either a fabric port (F_port) or fabric loop port (FL_port). See also *fabric port* and *fabric loop port.*

gateway. Hardware that connects incompatible networks by providing the necessary translation for both hardware and software.

GBIC. See *gigabit interface converter.*

Gbps. Gigabits per second.

GBps. Gigabytes per second.

generic port (G_port). A generic port that can operate as either an expansion port (E_port) or a fabric port (F_port). A port is defined as a G_port when it is not yet connected or has not yet assumed a specific function in the fabric.

gigabit interface converter (GBIC). A removable serial transceiver module designed to provide gigabaud capability for fibre channel (FC) and other products that use the same physical layer.

gigabit switch. A 16-port, Fibre Channel gigabit switch.

G_port. See *generic port.*

half duplex. A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time). See also *full duplex.*

hard address. The arbitrated loop physical address (AL_PA) that a node loop port (NL_port) attempts to acquire during loop initialization.

hardware translative mode. Method for achieving address translation. The two hardware translative modes that are available to a QuickLoop-enabled switch are standard translative mode and QuickLoop mode. See also *standard translative mode* and *QuickLoop mode.*

HBA. See *host bus adapter.*

heartbeat. Through clustering software, the application server continually communicates with the clustered spare using network heartbeats to indicate to the other machines that everything is operating correctly. This heartbeat is typically carried over a dedicated network for clustering traffic. In cases of a problem (for example, a software crash on the operational server or a hardware component failure), a heartbeat link indicates to the other server that something has failed or is otherwise inoperative. If that heartbeat is lost, the spare server takes over the function provided by the application service. Depending on the clustering software, either the entire server or only specific services on the server can be failed over or failed back.

high availability. An attribute of the switch that identifies it as being capable of operating well in excess of 99 percent of the time. High availability is typically identified by the number of nines in that percentage. For example, a switch that is rated at five nines would be capable of operating 99.999 percent of the time without failure.

high port count fabric. A fabric containing 100 or more ports.

host bus adapter (HBA). The interface card between a server or workstation bus and the Fibre Channel network.

hot pluggable. A field replaceable unit (FRU) capability that indicates it can be extracted or installed while customer data is otherwise flowing in the chassis.

hub. A Fibre Channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.

IC bus. A serial, 2-wire bus used to monitor field replaceable unit (FRU) temperatures and control the system including blade power control.

ID. Identification.

IDB. Interface descriptor block.

IDLE. Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

IEC. International Electrotechnical Commission.

IETF. Internet Engineering Task Force.

information unit (IU). A set of information as defined by either upper-level process protocol definition or upper-lever protocol mapping.

initiator. A server or workstation on a Fibre Channel network that initiates communications with storage devices. See also *target.*

in-order delivery (IOD). A parameter that, when set, guarantees that frames are either delivered in order or dropped.

integrated fabric. The fabric created by six switches cabled together and configured to handle traffic as a seamless group.

Internet protocol (IP). In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

inter-switch link (ISL). A Fibre Channel link that connects two switches (a link from the expansion port (E_port) of one switch to the E_port of another)

ROS nº 03/2005 - CN - CPMI - CORREIOS
1602
Fls. Nº
3690
Doc.

IOD. See *in-order delivery.*

IP. See *internet protocol.*

IPA. Initial process associator.

ISL. See *inter-switch link.*

ISL Trunking. A feature that enables distribution of traffic over the combined bandwidth of up to four inter-switch links (ISLs) (between adjacent switches), while preserving in-order delivery. A set of trunked ISLs is called a trunking group; each port employed in a trunking group is called a trunking port. See also *master port.*

isolated E_port. An expansion port (E_port) that is online but not operational between switches due to overlapping domain ID or nonidentical parameters such as error delay timeout values (E_D_TOVs). See also *expansion port.*

IU. See *information unit.*

K28.5. A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern. See also *comma.*

kernel flash. Flash memory that stores the bootable kernel code and is visible within the memory space of the processor. Data is stored as raw bits.

key pair. In public key cryptography, a pair of keys consisting of a public and private key of an entity. The public key can be publicized, but the private key must be kept secret.

LAN. See *local area network.*

latency. The period of time required to transmit a frame, from the time it is sent until it arrives.

LED. See *light-emitting diode.*

light-emitting diode (LED). A semiconductor chip that gives off visible or infrared light when activated.

link. As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibers. See also *circuit.*

link services. A protocol for link-related services.

LIP. See *loop initialization primitive.*

LM_TOV. See *loop master timeout value.*

local area network (LAN). A computer network located on a user's premises within a limited geographical area. (T)

logical unit number (LUN). An identifier used on a small computer systems interface (SCSI) bus to distinguish among up to eight devices (logical units) with the same SCSI ID.

long wavelength (LWL). A type of fiber optic cabling that is based on 1300 mm lasers and supports link speeds of 1.0625 Gbps. Can also refer to the type of GBIC or SFP. See also *short wavelength.*

loop. A configuration of devices that are connected to the fabric by way of a fabric loop port (FL_port) interface card.

loop circuit. A temporary bidirectional communication path established between loop ports (L_ports).

loop failure. Loss of signal within a loop for any period of time, or loss of synchronization for longer than the timeout value.

loop_ID. A hexadecimal value representing one of the 127 possible arbitrated loop physical address (AL_PA) values in an arbitrated loop.

loop initialization. The logical procedure used by a loop port (L_port) to discover its environment. Can be used to assign arbitrated loop physical address (AL_PA) addresses, detect loop failure, or reset a node.

loop initialization primitive (LIP). The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

looplet. A set of devices connected in a loop to a port that is a member of another loop.

loop master timeout value (LM_TOV). The minimum time that the loop master waits for a loop initialization sequence to return.

loop mode. One of the modes for a loop port (L_port). An L_port is in loop mode when it is in an arbitrated loop and is using loop protocol. An L_port in loop mode can also be in participating mode or nonparticipating mode. See also *loop port, fabric mode, participating mode,* and *nonparticipating mode.*

loop port (L_port). A node port (NL_port) or fabric port (FL_port) that has arbitrated loop capabilities. An L_port can be either in fabric mode or loop mode. See also *fabric mode , loop mode, nonparticipating mode,* and *participating mode.*

loop port state machine (LPSM). The logical entity that performs arbitrated loop protocols and defines the behavior of loop ports (L_ports) when they require access to an arbitrated loop.

L_port. See *loop port.*

LPSM. See *loop port state machine.*

LSR. Link state record.

LSU. Link state update.

LUN. See *logical unit number.*

LWL. See *long wavelength.*

MAC. Media access controller.

management information base (MIB). A simple network management protocol (SNMP) structure to help with device management, providing configuration and device information.

master port. As relates to trunking, the port that determines the routing paths for all traffic flowing through the trunking group. One of the ports in the first inter-switch link (ISL) in the trunking group is designated as the master port for that group. See also *ISL Trunking.*

MIB. See *management information base.*

modem serial port. The upper serial port on the control processor card (CP card) of the 2109 Model M12. Can be used to connect the CP card to a modem with a standard 9-pin modem cable. Consists of a DB-9 connector wired as an RS-232 device, and can be connected by serial cable to a data communications equipment (DCE) device. A Hayes-compatible modem or Hayes-emulation is required. The device name is ttyS1. See also *data communications equipment port* and *terminal serial port.*

multicast. The transmission of data from a single source to multiple specified node ports (N_ports), as opposed to all the ports on the network. See also *broadcast* and *unicast.*

multimode. A fiber optic cabling specification that allows up to 500 m (1640.5 ft) between devices.

name server. Frequently used to indicate Simple Name Server. See also *simple name server.*

NEMA. National Electrical Manufacturers Association.

NL_port. See *node loop port.*

NMS. Network Management System.

node. A Fibre Channel device that contains a node port (N_port) or node loop port (NL_port).

node loop port (NL_port). A node port that is loop capable. Used to connect an equipment port to the fabric in a loop configuration through a fabric loop port (FL_port).

node name. The unique identifier for a node, communicated during login and port discovery.

node port (N_port). A node port that is not loop capable. Used to connect an equipment port to the fabric.

nonparticipating mode. A mode in which a loop port (L_port) in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an arbitrated loop physical address (AL_PA) cannot be acquired. See also *participating mode.*

nonvolatile random access memory (NVRAM). Random access memory (storage) that retains its contents after the electrical power to the machine is shut off. A specific part of NVRAM is set aside for use by the system ROS for the boot device list.

N_port. See *node port.*

NVRAM. See *nonvolatile random access memory.*

Nx_port. A node port that can operate as either a node port (N_port) or node loop port (NL_port). See also *node port* and *node loop port.*

operating system (OS). A collection of system programs that control the overall operation of a computer system.

ordered set. A transmission word that uses 8b/10b mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include frame delimiters, primitive signals, and primitive sequences. Ordered sets are used to differentiate Fibre Channel control information from data frames and to manage the transport of frames. See also *frame delimiter*, *primitive signal*, and *primitive sequence.*

OS. See *operating system.*

packet. A set of information transmitted across a network. See also *frame.*

participating mode. A mode in which a loop port (L_port) in a loop has a valid arbitrated loop physical address (AL_PA) and can arbitrate, send frames, and retransmit received transmissions. See also *nonparticipating mode.*

path selection. The selection of a transmission path through the fabric. Switches use the Fibre Channel shortest path first (FSPF) protocol.

PCI. Peripheral control interconnect.

PDU. Power distribution unit.

Performance Monitoring. A feature that provides error and performance information to the administrator and user for use in storage management.

phantom address. An arbitrated loop physical address (AL_PA) value that is assigned to a device that is not physically in the loop. Also known as phantom AL_PA.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1603
Fls. Nº
3650
Doc:

phantom device. A device that is not physically in an arbitrated loop, but is logically included through the use of a phantom address.

PLDA. See *private loop direct attach.*

PLOGI. See *port login.*

PMC. PCI mezzanine card.

P/N. Part number.

point-to-point. A Fibre Channel topology that employs direct links between each pair of communicating entities.

port cage. The metal casing extending out of the optical port on the switch, and in which the gigabit interface converter (GBIC) or small form-factor pluggable (SFP) can be inserted.

port card. A Fibre Channel card that contains optical or copper port interfaces, and acts like a switch module. See also *16-port card.*

port login (PLOGI). The port-to-port login process by which initiators establish sessions with targets. See also *fabric login.*

port module. A collection of ports in a switch.

port_name. The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST. See *power-on self-test.*

power-on self-test (POST). A series of diagnostics that are automatically run by a device when the power is turned on.

primary FCS switch. Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric. See also *backup FCS switch* and *FCS switch.*

primitive sequence. A part of an ordered set that indicates or initiates port states. See also *ordered set.*

primitive signal. A part of an ordered set that indicates events. See also *ordered set.*

principal switch. The switch that assumes the responsibility to assign domain IDs. The role of principal switch is negotiated after a "build fabric" event.

private device. A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.

private loop. An arbitrated loop that does not include a participating fabric loop port (FL_port).

private loop direct attach (PLDA). A subset of fibre channel standards for the operation of peripheral devices.

private NL_port. A node loop port (NL_port) that communicates only with other private NL_ports in the same loop and does not log into the fabric.

protocol. A defined method and a set of standards for communication.

public device. A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.

public loop. An arbitrated loop that includes a participating fabric loop port (FL_port), and can contain both public and private node loop ports (NL_ports).

public NL_port. A node loop port (NL_port) that logs into the fabric, can function within either a public or private loop, and can communicate with either private or public NL_ports.

quad. A group of four adjacent ports that share a common pool of frame buffers.

QuickLoop. (1) A feature that makes it possible to allow private devices within loops to communicate with public and private devices across the fabric through the creation of a larger loop. (2) The arbitrated loop created using this software. A QuickLoop can contain a number of devices or looplets; all devices in the same QuickLoop share a single arbitrated loop physical address (AL_PA) space.

QuickLoop mode. A hardware translative mode that allows private devices to communicate with other private devices across the fabric. See also *hardware translative mode* and *standard translative mode.*

RAID. See *redundant array of independent disks.*

RAM. See *random access memory.*

RAN. Remote Asynchronous Notification.

random access memory (RAM). A temporary storage location in which the central processing unit (CPU) stores and executes its processes.

R_A_TOV. See *resource allocation timeout value.*

read only memory (ROM). Memory in which stored data cannot be changed by the user except under special conditions.

receiver ready (R_RDY). A primitive signal indicating that the port is ready to receive a frame.

reduced instruction set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid processing.

redundant array of independent disks (RAID). A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

registered state change notification (RSCN). A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.

remote fabric. A fabric that spans across wide area networks (WANs) by using protocol translation (a process also known as tunneling) such as fibre channel over asynchronous transfer mode (ATM) or fibre channel over Internet protocol (IP).

remote procedure call (RPC). A facility that a client uses to request the execution of a procedure call from a server.

Remote Switch. A feature that runs on Fabric operating system (OS) and enables two fabric switches to be connected over an asynchronous transfer mode (ATM) connection. This requires a compatible Fibre Channel to ATM gateway, and can have a distance of up to 10 km (6.214 mi) between each switch and the respective ATM gateway.

request rate. The rate at which requests arrive at a servicing entity. See also *service rate.*

resilient core. A single fabric that uses two or more switches as a core to interconnect multiple edge switches. Synonymous with dual-core fabric.

resource allocation timeout value (R_A_TOV). Used to time out operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered. This value is adjustable in one microsecond increments from 10 - 120 seconds.

resource recover timeout value (RR_TOV). The minimum time a target device in a loop waits after a loop initialization primitive (LIP) before logging out a small computer systems interface (SCSI) initiator. See also *error detect timeout value* and *resource allocation timeout value.*

RISC. See *reduced instruction set computer.*

RLS probing. Read link status of the arbitrated loop physical addresses (AL_PAs).

ro. Read only.

ROM. See *read only memory.*

route. As applies to a fabric, the communication path between two switches. Can also apply to the specific path taken by an individual frame, from source to destination. See also *Fibre Channel shortest path first.*

routing. The assignment of frames to specific switch ports, according to frame destination.

RPC. See *remote procedure call.*

R_RDY. See *receiver ready.*

RR_TOV. See *resource recovery timeout value.*

RS-232 port. A port that conforms to a set of Electrical Industries Association (EIA) standards. Used to connect data terminal equipment (DTE) and data communications equipment (DCE) devices for communication between components, terminals, and modems. See also *DB-9 connector, DCE port,* and *DTE port.*

RSCN. See *registered state change notification.*

RSH. Remote shell.

RTC. Real time clock.

rw. Read-write.

SAN. See *storage area network.*

SAN island. A group of storage devices and servers connected to switches in a fabric.

SC. Standard connector.

SCSI. See *small computer systems interface.*

SCSI Enclosure Services (SES). A subset of the small computer systems interface (SCSI) protocol used to monitor temperature, power, and fan status for enclosure devices.

SDRAM. See *synchronous dynamic random access memory.*

Secure Fabric OS. An optionally-licensed software product that runs on top of the Fabric OS and provides customizable security restrictions through local and remote management channels on a switch.

secure sockets layer (SSL). A security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

sequence. A group of related frames transmitted in the same direction between two node ports (N_ports).

SERDES. Serializer/deserializer.

service rate. The rate at which an entity can service requests. See also *request rate.*

SES. See *SCSI Enclosure Services.*

SFP. See *small form-factor pluggable.*

short wavelength (SWL). A type of fiber optic cabling that is based on 850 mm lasers and supports 1.0625 Gbps link speeds. Can also refer to the type of gigabit

Fls. Nº 1804
Doc: 3690

interface converter (GBIC) or small form-factor pluggable (SFP). See also *long wavelength.*

SID. The 3-byte source ID of the originator device, in the 0xDomainAreaALPA format.

SID-DID. Source identifier-destination identifier.

SIMMS. Single in-line modules.

simple name server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Can also be referred to as directory service. See also *Fibre Channel service.*

simple network management protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

single mode. The fiber optic cabling standard that corresponds to distances of up to 10 km (6.214 mi) between devices.

small computer systems interface (SCSI). A parallel bus architecture and a protocol for transmitting large data blocks up to a distance of 15 - 25 m (49 - 82 ft).

small form-factor pluggable (SFP). An optical transceiver used to convert signals between optical fiber cables and switches.

SMI. Special memory interface.

SNIA. Storage Network Industry Association.

SNMP. See *simple network management protocol.*

SNMPv1. The original standard for SNMP, now labeled v1.

SNS. See *simple name server.*

SOF. Start-of-frame.

SSL. See *secure sockets layer.*

standard translative mode. A hardware translative mode that allows public devices to communicate with private devices across the fabric. See also *hardware translative mode* and *QuickLoop mode.*

storage area network (SAN). A network of systems and storage devices that communicate using Fibre Channel protocols. See also *fabric.*

subordinate switch. All switches in the fabric other than the principal switch. See also *principal switch.*

switch. Hardware that routes frames according to Fibre Channel protocol and is controlled by software.

switch name. The arbitrary name assigned to a switch.

switch port. A port on a switch. Switch ports can be expansion ports (E_ports), fabric ports (F_ports), or fabric loop ports (FL_ports).

SWL. See *short wavelength.*

synchronous dynamic random access memory (SDRAM). The main memory for the switch. Used for volatile storage during switch operation.

Tachyon. A type of host bus adapter.

target. A storage device on a Fibre Channel network. See also *initiator.*

TCP. See *transmission control protocol.*

tenancy. The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.

terminal serial port. The lower serial port on the control processor card (CP card) of the 2109 Model M12. This port sends switch information messages and can receive commands. Can be used to connect the CP card to a computer terminal. Has an RS-232 connector wired as a data terminal equipment (DTE) device, and can be connected by serial cable to a data communications equipment (DCE) device. The connector pins 2 and 3 are swapped so that a straight-through cable can be used to connect to a terminal. The device name is ttyS0. Can also be referred to as the console port. See also *DCE port, DTE port,* and *modem serial port.*

throughput. The rate of data flow achieved within a cable, link, or system. Usually measured in bits per second (bps). See also *bandwidth.*

topology. As applies to fibre channel, the configuration of the Fibre Channel network and the resulting communication paths allowed.

translative mode. A mode in which private devices can communicate with public devices across the fabric.

transmission character. A 10-bit character encoded according to the rules of the 8b/10b algorithm.

Transmission Control protocol (TCP). A communications protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for Internet protocol.

transmission word. A group of four transmission characters.

trap (SNMP). The message sent by a simple network management protocol (SNMP) agent to inform the SNMP management station of a critical error. See also *simple network management protocol.*

tunneling. A technique for enabling two networks to treat a transport network as though it were a single communication link or local area network (LAN).

Tx. Transmitted.

U. Unit of measure for rack-mounted equipment.

UART. Universal Asynchronous Receiver Transmitter.

UDP. See *user datagram protocol.*

ULP. See *upper-level protocol.*

ULP_TOV. See *upper-level timeout value.*

unicast. The transmission of data from a single source to a single destination. See also *broadcast* and *multicast.*

universal port (U_port). A switch port that can operate as a generic port (G_port), expansion port (E_port), fabric port (F_port), or fabric loop port (FL_port). A port is defined as a U_port when it is not connected or has not yet assumed a specific function in the fabric.

U_port. See *universal port.*

upper-level protocol (ULP). The protocol that runs on top of Fibre Channel. Typical upper-level protocols are small computer system interface (SCSI), Internet protocol (IP), HIPPI, and IPI.

upper-level timeout value (ULP_TOV). The minimum time that a small computer system interface (SCSI) upper-level protocol (ULP) process waits for SCSI status before initiating ULP recovery.

user datagram protocol (UDP). A protocol that runs on top of Internet protocol (IP) and provides port multiplexing for upper-level protocols.

user flash. See *compact flash.*

VC. See *virtual circuit.*

VCCI. Voluntary Control Council for Interference

virtual circuit (VC). A one-way path between node ports (N_ports) that allows fractional bandwidth.

WAN. See *wide area network.*

WDM. Wave division multiplexing.

well-known address. As pertaining to fibre channel, a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan network, and that can use or provide public communications facilities. (T)

workstation. A computer used to access and manage the fabric. Can also be referred to as a management station or host.

worldwide name (WWN). Uniquely identifies a switch on local and global networks.

World Wide Web (WWW). A network of servers that contain programs and files. Many of the files contain hypertext links to other documents available through the network.

WWN. See *worldwide name.*

WWW. See *World Wide Web.*

XLWL. See *extra long wavelength.*

zone. A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone. See also *zoning.*

zone alias. An alias for a set of port numbers or worldwide names (WWNs). Zone aliases can be used to simplify the entry of port numbers and WWNs. For example, "host" could be used as an alias for a WWN of 110:00:00:60:69:00:00:8a.

zone configuration. A set of zones designated as belonging to the same zone configuration. When a zone configuration is in effect, all valid zones in that configuration are also in effect.

zone member. A port, node, worldwide name (WWN), or alias, which is part of a zone.

zone scheme. The level of zoning granularity selected. For example, zoning can be done by switch or port, worldwide name (WWN), arbitrated loop physical address (AL_PA), or a mixture. See also *zone configuration.*

zone set. See *zone configuration.*

Zoning. A feature that runs on Fabric operating system (OS) and allows partitioning of the fabric into logical groupings of devices. Devices in a zone can only access and be accessed by devices in the same zone. See also *zone.*

CORREIOS
1605
3690
Doc:

Index

Numerics

16-port card specifications 18
2109 Model C36 with Model M12 library xv
2N power architecture 8

A

about this document
  related publications xv
  who should read this document xv
ac input 8
address
  director of licensing 51
  IBM xvii
Advanced Security feature 13

B

battery notice xiv
battery specifications 19
Brocade
  documents xv
  IBM product and model number matrix xvi

C

cable
  management 7
  side, LEDs 12
caution notices
  battery xiv
  customer setup xi
  example xi
  laser safety xiii
  linecord xii
  translations 27
certification, safety 25
checking safety labels xi
Chinese Class A compliance statement 52
Class 1 laser product xiii
comments, how to send xvii
compliance, regulatory 25
components
  switch 17
  weight 17
configuration, CP blade assembly 10
cooling system 6
CP blade assembly
  configuration 10
  description 9
  management 10
CPU subsystem 9
customer setup caution notice xi

D

danger notices
  electrical outlet xi
  example xi
  translations 27
dc outputs 8
design
  high availability 4
  overview 3
  switch blade assembly 11
diagnostic tests 12
dimensions of the switch 17
director of licensing, address 51
disposal, product xiv

E

electronic emission statements 52
EMC (electromagnetic compatibility) 25
EMI (electromagnetic interference) 25
environmental
  notices xiii
  requirements 22
Ethernet ports 5
European Community compliance statement 53
Extended Fabrics 13

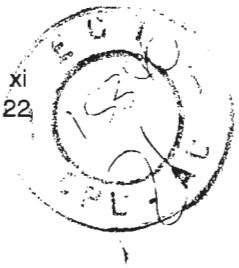
F

Fabric Manager 14
Fabric OS
  description 14
facility specifications 20
fault monitoring and diagnostics 12
FCC
  emission limits 52
  rules 52
  statement 52
FDA 21 CFR 1040.10 and 1040.11 xiii
features
  Advanced Zoning 14
  Fabric Watch 14
  ISL Trunking 14
  Performance Monitoring 14
  software 13
    Advanced Security 13
    Extended Fabrics 13
    Fabric Manager 14
    Fabric OS 13
    Remote Switch 13
  Web Tools 14
Federal Communications Commission (FCC)
 statement 52
Fibre Channel Association Web site xvi
field replaceable units 16
fire suppression systems xiv

© Copyright IBM Corp. 2002, 2003

CPMI - CORREIOS
Fls. Nº 1606
3690
Doc:

form
reader comment, how to send xvii
FRUs (field replaceable units) 16



G

GBIC label on the 2109 Model M12 xi
general specifications of the switch 22
Germany compliance statement 53
getting
help xvi
software updates xvi

H

help, getting xvi
high availability design 4
how to send your comments xvii

I

IBM
address xvii
director of licensing, address 51
trademarks 52
IBM product and model number matrix xvi
IEC 825-1 xiii
immunity 26
indicators, system status 12
Industry Canada compliance statement 52
intellectual property 51
interference, radios and televisions 52
interoperability, description 15
introduction 1

J

Japanese Voluntary Control Council for Interference (VCCI) class 1 statement 54

K

Korean Government Ministry of Communication (MOC) statement 54

L

label
check, safety xi
laser safety caution xii, xiii
linecord caution xii
safety xiii
SFP xii
laser safety xiii
LEDs
cable-side 12
card 7
noncable side 13
license for patents 51
linecord caution label xii, xiii
link distance, high-speed Fibre Channel switch 2

M

management
cable 7
CP blade assembly 10
materials, recyclable xiv
memory specifications 19
modem serial port specifications 20

N

network manageability 15
noncable side LEDs 13
notices
caution, battery xiv
edition ii
environmental xi, xiii
example of caution xi
example of danger xi
IBM 51
safety xi
safety translation xi
numbering 6

O

optical port
description 5
terminators xiii
overview
product 1
system design 3

P

patents 51
port
description 5
Ethernet 5
optical 5
serial 6
switch 17
power distribution system
specifications 7
strategy 8
power specifications of the switch 21
product
disposal xiv
overview 1
recycling xiv
specifications 18
publications
2109 Model C36 with Model M12 library xv
Web sites xvi

R

rack mounting 6
radio interference 52
reader comment form processing xvii
recycling products xiv
regulatory
  compliance 25
  specifications 23
related documents xv
reliability 4
Remote Switch 13
requirements, environmental 22
restrictions, usage xiii

S

safety
  certifications 25
  label xi
  label checks xi
  laser xi, xiii
  notice translations xi
  notices xi
  product disposal xiv
security, description 15
sending your comments xvii
serial ports 6
serviceability 5
SFP
  description 2
  label xii
small form factor pluggable optical fiber optic transceivers 2
software
  features 13
    Advanced Security 13
    Advanced Zoning 14
    Extended Fabrics 13
    Fabric Manager 14
    Fabric OS 13
    Fabric Watch 14
    ISL Trunking 14
    Performance Monitoring 14
    Remote Switch 13
    Web Tools 14
  getting updates xvi
specifications
  16-port card 18
  battery 19
  facility 20
  general 22
  memory 19
  modem serial port 20
  power 21
  product 18
  regulatory 23
  terminal serial port 19
statements
  Chinese Class A compliance 52
  electronic emission 52
statements *(continued)*
  European Community compliance 53
  Federal Communications Commission 52
  Germany compliance 53
  Industry Canada compliance 52
  Japanese Voluntary Control Council for Interference (VCCI) class 1 54
  Korean Government Ministry of Communication (MOC) 54
  Taiwan class A compliance 54
strategies, power distribution 8
subsystem, CPU 9
switch
  components 17
  dimensions 17
  overview 1
  ports 17
  specifications
    facility 20
    general 22
    memory 19
    modem serial port 20
    power 21
    regulatory 23
    terminal serial port 19
  weight 17
switch blade assembly
  description 11
  design 11
system
  cooling 6
  design, overview 3
  fabric operating 14
  fire suppression xiv
  power distribution 7
  status indicators 12

T

Taiwan class A compliance statement 54
take-back program, product xiv
terminal serial port specifications 19
terminators for optical ports xiii
tests, diagnostic 12
throughput, high-speed Fibre Channel switch 2
trademarks 52
transceivers, SFP 2
translations, danger and caution notices 27

U

unauthorized changes or modifications 52
updates, getting software xvi
usage restrictions xiii

V

voltage label xiii

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1607
Doc. 3690

W

Web sites xvi
weight of the switch and components 17
who should read this document xv

Readers' comments — we would like to hear from you.

IBM TotalStorage SAN Switch
2109 Model M12 User's Guide

Publication No. GC26-7468-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

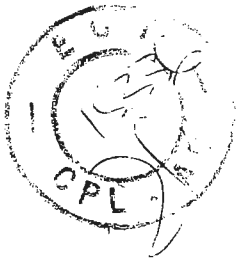
Phone No.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1608
Doc: 3656

Readers' Comments — We'd Like to Hear from You
GC26-7468-02

IBM®

Cut or Fold
Along Line



Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
RCF Processing Department
Dept. M86/Bldg.050-3
5600 Cottle Road
San Jose, CA
U.S.A. 95193-0001

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1609
Doc: 3690

Spine information:

IBM TotalStorage SAN Switch 2109 Model M12 User's Guide

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1610
Doc: 3690

Manual 08

3583 Ultrium Scalable Tape Library

Interoperability Matrix

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1611
3690
Doc:

3583 Ultrium Scalable Tape Library

Interoperability Matrix (List of Supported Servers)

Last Update Date: 5/06/03

Midrange and Open Systems Connectivity

IBM's TotalStorage Ultrium Scalable Tape Library 3583 provides a single storage solution designed t provide superior performance for many hardware and software systems.

Supported Independent Software (ISV) Vendors
Get the latest firmware and device drivers.

Supported Servers

Hewlett-Packard Servers
IBM iSeries and AS/400 Servers
IBM pSeries, RS/6000 and SP Servers
Microsoft Windows Servers
SUN Servers
Linux Support

Open Systems Support

The supported open systems environments are shown below. The sales representative and/or customer responsible for insuring that the specific host system configuration used (i.e. server model, operating system level and host adapter combination) is a valid and supported configuration.

Note:
IBM development plans are subject to change or withdrawal at any time without prior notice.

Hewlett-Packard Servers

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
HP 9000 Series	**HP-UX**	**HP**

CPMI - CORREIOS
Fls. Nº 1612
Doc: 3690

rp2400), L (rp5400), N 7400) Class N Class	11.0 11.i	HP4800A (PCI)HVD Ultra; HP5149A (PCI) LVD Ultra2; HP5150A (PCI) LVD Ultra2

tes

1. For V Class Servers, adapter 4800A requries the inline HVD SCSI terminator, Feature 5098.
2. The 3rd edition (E1298) of the HP Service and User's Guide for the 4800A PCI Ultra SCSI HBA specifies support for HP V22xx and V25xx Servers. Support for V2600 is not documented although the V2500/V2600 System Upgrade Guide (1st Edition) does not mention any adapter incompatibilities.
3. The 5150A PCI to Ultra 2 SCSI HBA Service and User Guide (2nd Edition, 2001) does not indicate support for V Class Systems - only N and L Class.
4. The 5149A PCI to Ultra 2 SCSI HBA Service and User Guide (2nd Edition, 2001) indicates support for V Class systems including the V2600 under HP-UX 11.0 and 11i. For V Class systems attach, HP specifies the 5M V-Class SE/LVD inline termination cable.

ore Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models

rvers	Operating Systems	Host Adapters/SAN
9000 Series	**HP-UX**	**HP**
rp2400), L (rp5400), N 7400) Class N Class	11.0 patch PHKL 21834 for N-Class; patch PHKL 22903 for L-Class 11.i	Click Here for details.

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultium Scalable Tape Library
2. For Details and guidelines click here.

M @server iSeries and AS/400 Servers

SI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models

rvers	Operating Systems	Host Adapters
rvers that support the ted host adapters.	**OS/400** V5R1, V5R2	FC 6501[1] HVD (Ultrium 1 Only); FC 6534 HVD; FC 2729 HVD Ultra PCI; FC 2749 HVD Ultra PCI; FC 5702 LVD Ultra PCI [2] (Ultrium 2 Only)

tes

(1) Interposer for AS/400 Feature # 6501(Feature code 2895 on the 3583 Ultrium Tape Library)
(2) Requires V5R2

(3) For D-mode IPL, the device SCSI address must be set tp "0"

(4) One iSeries host and one device per SCSI 3583

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters/SAN**
Servers that support the listed host adapters.	**OS/400** V5R1, V5R2	Click here for details.

Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feat 8005 in 3583 Ultrium Scalable Tape Library.
2. The iSeries Fibre Channel attach supports multiple hosts and maximum six drive configuration for the 3583 Feature 8005 device.

D-mode IPL is not supported with Fibre Channel attached tape drives. The Alternate Installatic Device (Boot Manager) support must be used.

Note: You will need to order the appropriate feature(s) to your 3583 Ultrium Scalable Tape Library.

IBM @server pSeries and RS/6000 and RS/6000 SP Servers

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
Servers that support the listed host adapters.	**AIX** 4.3.3 and Higher	**IBM** FC 6204 HVD Ultra PCI; FC 6207 HVD Ultra PCI; FC 6205 LVD Ultra2 PCI; FC 6203 LVD/SE Ultra3 (PCI); Integrated Ultra2 SCSI LVD with VHDCI[1]; Integrated Ultra3 SCSI LVD with VHDCI[2]
Notes		

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1613
Doc: 3690

ease check with the sales representatives for specific host adapters supported by model and detailed achment and configuration information

1. Integrated LVD adapter with AIX 4.3.3 or higher on 7044 models 170 & 270, pSeries 620 (7025-6F1) & (7025-6F0), 7025 model F80, pSeries 640 (7026-B80), pSeries 660 (7026-6H1) & (7026-6H0) & (7026-6M1), 7026 models H80 & M80. For **6203 & 6204**, pSeries 670 (7040-671) through I/O drawer (7040-61D), pSeries 690 (7040-681) through I/O drawer (7040-61D), 9112-265.
2. Integrated Ultra 3 SCSI LVD adapter with AIX 4.3.3 or higher on pSeries 610 (7028-6C1) & (7028-6E1), 9112-265.
3. AIX 5.1 requires Atape driver level 6.1.4.0 or above; Level 7.0.6.0 or above recommended for the latest Ultrium timeout values.

bre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
rvers	Operating Systems	Host Adapters/SAN
rvers that support the ted host adapters.	**AIX** 4.3.3 and Higher	Click here for details.

otes

ease check with the sales representatives for specific host adapters supported by model and detailed achment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.
2. AIX 5.1 requires Atape driver level 6.1.4.0 or above; Level 7.0.6.0 or above recommended for the latest Ultrium timeout values

icrosoft Windows NT, 2000, and 2003 Support

CSI Ultrium LVD Ultrium 1 & Ultrium 2 and HVD Drive Models		
rvers	Operating Systems	Host Adapters
rvers that support ted host adapters.	NT Server V4 with SP 6 (Ultrium 1 Only today) or Windows 2000 Build 2195 Or Windows 2003 Build 3790	Adaptec AHA 2944 UW HVD Ult (PCI), Netfinity Adapter #59H3900 HVD Ultra; Adaptec 29160 LVD Ultra160 PCI [1]; Adaptec 39160 LVD Ultra160 PCI [1]; Adaptec 2940 U2B LVD Ultra2 PCI or Netfinity Adapter #33L5000 Ultra2 SCSI PCI; Netfinity Adapter #19K4646 or Adaptec 29160LP [1&2]; Adaptec 39320 LVD Ultra320 PCI ——— LSI Logic Sym 22910 LVD Ultra2 PCI

otes

1. **Supported with Restrictions.** See ftp://ftp.software.ibm.com/storage/devdrvr/Windows/Win2000/IBMUltrium.Win2K.Readme.t or ftp://ftp.software.ibm.com/storage/devdrvr/Windows/Win2003/IBMUltrium.W2K3.Readme or ftp://ftp.software.ibm.com/storage/devdrvr/Windows/WinNT/IBMUltrium.Win2K.Readme. for instructions.
2. Netfinity Adapter #19K4646 SCSI PCI Adapter made by Adaptec for IBM Netfinity.
3. See the Host Bus Adapter Supported Fibre Versions Matrix for the latest HBA support information, and the LTO Device Drivers for the latest device driver downloads.

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters/SAN**
Servers that support the listed host adapters.	NT Server V4 with SP6A or later (SDG 8005 with Ultrium 1 Only at this time) or Windows 2000 Build 2195 Or Windows 2003 Build 3790	Click here for details.

Notes

Please check with the sales representatives for specific host adapters supported by model and detailed attachment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or featu 8005 in 3583 Ultrium Scalable Tape Library.

SUN Systems

SCSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models		
Servers	**Operating Systems**	**Host Adapters**
SUN SPARC, UltraSPARC, and **Ultra/Enterprise Servers** that support the listed host adapters.	**Solaris** 7, 8, and 9	**SUN** X1065A HVD Ultra Sbus; X6541A [1] HVD Ultra PCI; X2222A LVD Ultra PCI

Notes

1. SUN Adapter X 6541 requires a VHDC1 interposer/cable; feature code 5099 on the 3583.

Fibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models		
Servers	**Operating Systems**	**Host Adapters**

15328
CPMI - CORREIOS
Fls. Nº 1614
3690
Doc:

JN SPARC, UltraSPARC, d Ultra/Enterprise rvers that support the listed st adapters.	**Solaris** 7, 8, and 9	Click here for details.

otes

ease check with the sales representatives for specific host adapters supported by model and detailed achment and configuration information

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or feature 8005 in 3583 Ultrium Scalable Tape Library.

inux Support

CSI LTO Ultrium 1 & Ultrium 2 LVD and HVD Drive Models

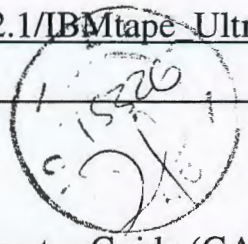
ervers	Operating Systems	Host Adapters
2-bit Intel based	RedHat 7.2 with kernel 2.4.9-31 (Ultrium1 Only) RedHat 7.3 (Ultrium 1 Only) Advanced Server 2,1; SuSE Linux Enterprise Server 7 Update	LVD: Adaptec AHA 2944 UW; HVD: Adaptec 29160[3]; HVD Adaptec 39160[3]; HVD Adaptec 2940 U2W

ibre Channel LTO Ultrium 2 Drive or SAN Data Gateway Module Feature 8005 Models

ervers	Operating Systems	Host Adapters/SAN
2-bit Intel based	RedHat 7.2 with kernel 2.4.9-31 (SDG & Ultrium 1 Only); RedHart 7.3 (Ultrium 1 Only); RedHat Advanced Server 2.1; SuSE Linus Enterprise Server 7 Update	Click here for details
4-bit Intel based	RedHat Advanced Server 2,1 (SDG & Ultrium1 Only);	Click here for details

Notes

1. Fabric Support is only supported by the LTO Ultrium Fibre Channel Drive feature 8105 or featur 8005 in 3583 Ultrium Scalable Tape Library.
2. For more details on IBM tape device drivers and drive microcode levels click here.
3. **Supported with Restrictions.** See ftp://ftp.software.ibm.com/storage/devdrvr/Linux/RHLAS2.1/IBMtape_Ultrium.Readme.txt for instructions.



dditional Product Information is available:

3M TotalStorage Ultrium Scalable Tape Library 3583 Setup, Operator Guide (GA32-0411).

he 3583 Ultrium Scalable Tape Library is supported by a variety of applications from Independent oftware Vendors.

eneral Notes:

tachment of LTO Ultrium 2 Tape Drives with the Adaptec SCSI Card 29160 or Adaptec 39160, installed in 32 bit PCI slots, is not supported.

ll mation on this page is provided by IBM on an "AS IS" basis only. IBM provides no warranty of compatibility. dividual results may vary based on environment.

se of information that is provided by IBM is at the recipient's own risk. IBM provides no assurances that any reported oblems may be resolved with the use of any information that IBM provides. By furnishing information, IBM does not ant any licenses to any copyrights, patents or any other intellectual property rights.

) International Business Machines Corporation 2003.

ny trademarks and product or brand names referenced in this document are the property of their respective owners. Plea nsult your IBM product manuals for complete trademark information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 1615
Doc: 3690

Manual 09

IBM Tivoli
Storage Area Network Manager
Guia do Usuário Versão 1 Release 2

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1616
3690
Doc:

IBM Tivoli Storage Area Network Manager

Guia do Usuário

Versão 1 Release 2

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1617
Doc: 3690

SC17-7576-01

- Dê um clique duplo no símbolo do host, no painel à direita, para exibir o sistema operacional.
- Dê um clique duplo no símbolo do sistema operacional, no painel á direita, para exibir os sistemas de arquivos.

Exibindo as Propriedades do Dispositivo da SAN

O Tivoli Storage Area Network Manager armazena as informações que ele descobre sobre os dispositivos na SAN. Para acessar essas informações, clique no símbolo do dispositivo no submapa e selecione **SAN → SAN Properties** no menu do console. A Figura 18 mostra como selecionar as propriedades de uma chave Fibre Channel denominada **SRMSW4**.

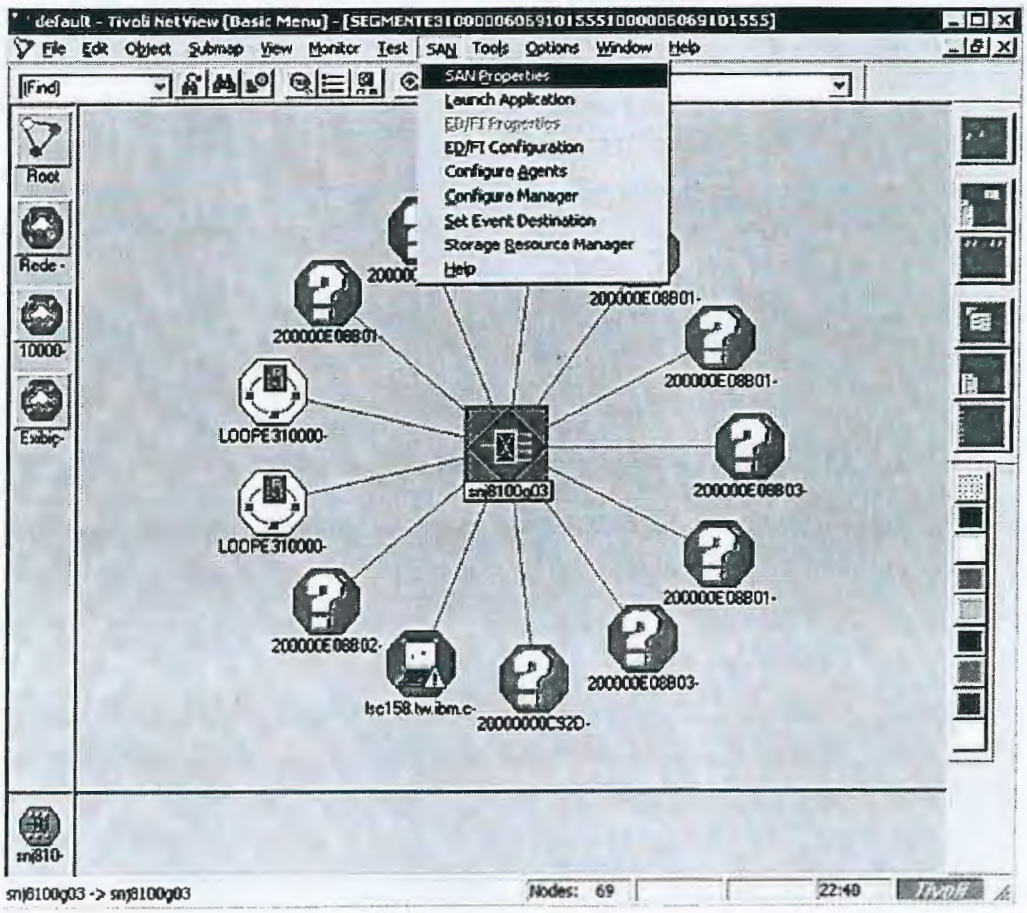


Figura 18. Exibindo propriedades do dispositivo da SAN

A Figura 19 na página 30 mostra as propriedades do comutador. Se você selecionou um dispositivo de armazenamento, veria as propriedades exclusivas desse dispositivo de armazenamento. Para obter informações detalhadas sobre os campos de propriedades exibidos, clique no botão **Ajuda**, no canto inferior direito da exibição de propriedades.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls Nº 1618
Doc: 3690