Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Release Notes, Cisco IOS Release 12.2(37)SE and Later

Revised August 8, 2007

These release notes include important information about this Cisco IOS release for the Cisco Gigabit Ethernet Switch Module (CGESM) for the HP BladeSystem p-Class. This document includes any limitations, restrictions, and caveats that apply to this release.

To verify that these release notes are correct for your switch, use the **show version** user EXEC command (see the "Finding the Software Version and Feature Set" section on page 3).

You can download the switch software from this URL:

http://www.hp.com/support

Contents

This information is in the release notes:

© 2005-2007 Hewlett-Packard Development Company, L.P.

System Requirements

The system requirements are described in these sections:

Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

Hardware Requirements

Table 1 lists the minimum hardware requirements for running the device manager.

Table 1 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II[1]	64 MB[2]	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

Software Requirements

Table 2 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

Note The device manager does not require a plug-in.

Table 2 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI).

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a CGESM switch, all standby command switches must be CGESM switches.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- "Finding the Software Version and Feature Set" section on page 3
- "Deciding Which Files to Use" section on page 4
- "Upgrading a Switch by Using the Device Manager" section on page 4
- "Upgrading a Switch by Using the CLI" section on page 4
- "Recovering from a Software Failure" section on page 5

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** user EXEC command to display the software version that is running on your switch.

You also can use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Here are the filenames for this software release:

- cgesm-lanbase-tar.122-37.SE1.tar
- cgesm-lanbasek9-tar.122-37.SE1.tar

Upgrading a Switch by Using the Device Manager

You can upgrade switch software by using the device manager. From the feature bar, choose **Administration > Software Upgrade**. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image. The **archive download-sw** privileged EXEC command both downloads and extracts the files.

To download the image for a CGESM switch, follow these steps:

Step 1 Go to: http://www.hp.com/support and select the appropriate country or region.

Step 2 From the Support and Drivers page, click the **Download drivers and software (and firmware)** radio button.

Step 3 Enter **CGESM** in the product field and press the **Right Arrow** key.

Step 4 Select an operating system, then click on the desired blade infrastructure or firmware release.

Step 5 Click the **download** button to download the image.

To download the cryptographic software files, click the software depot link in the Notes section. Once there, search for CGESM or go to the Enhancement releases and patch bundles section.

Step 6 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 7 Log into the switch through the console port or a Telnet session.

Step 8 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

Step 9 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

archive download-sw /overwrite /reload tftp:[[*//location*]*/directory*]*/image-name***.tar**

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For ***//****location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/cgesm-i612-tar.122-25.SE1.tar
```

You also can download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For recovery procedures, see the "Troubleshooting" chapter in the *Cisco Gigabit Ethernet Switch Module for HP-Blade System p-Class Software Configuration Guide* for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the *Cisco Gigabit Ethernet Switch Module for HP-Blade System p-Class Hardware Installation Guide*.
- The CLI-based setup program, as described in the *Cisco Gigabit Ethernet Switch Module for HP-Blade System p-Class Hardware Installation Guide*.
- The DHCP-based autoconfiguration, as described in the *Cisco Gigabit Ethernet Switch Module for HP-Blade System p-Class Software Configuration Guide*.
- Manually assigning an IP address, as described in the *Cisco Gigabit Ethernet Switch Module for HP-Blade System p-Class Software Configuration Guide*.

New Software Features

- VLAN Flex Links load balancing to configure a Flex Links pair to allow both ports to forward traffic for some VLANs (mutually exclusive)
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones
- VLAN aware port security option to shut down the VLAN on the port when a violation occus, instead of shutting down the entire port
- DHCP snooping statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form
- SNMP support for the Port Error Disable MIB
- Support for the Time Domain Reflectometry MIB

Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release required to support the major features on this switch.

Table 3 CGESM Switch Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
VLAN Flex Links load balancing	12.2(37)SE
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE
VLAN aware port security	12.2(37)SE
Support for DHCP snooping statistics	12.2(37)SE
Support for auto rendezvous point (auto-RP) for multicast	12.2(37)SE
Web authentication	12.2(35)SE
Support for DSCP transparency	12.2(25)SE1
Support for VLAN-based QoS and hierarchical policy maps on SVIs	12.2(25)SE1
Device manager	12.2(25)SE1
Support for SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE1
802.1x accounting and MIBs (IEEE8021-PAE-MIB and CISCO-PAE-MIB)	12.2(25)SE1
Flex Links	12.2(25)SE1
HTTP software upgrade (device manager only)	12.2(25)SE1
SFP module diagnostic-management interface	12.2(25)SE1
Smartports macros	12.2(25)SE1

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

Cisco IOS Limitations

These limitations apply to CGESM switch:

Configuration

These are the configuration limitations:

- If you run the CLI-based setup program, the IP address that the Dynamic Host Configuration Protocol (DCHP) provides is reflected as a static IP address in the config.text file. The workaround is to not run setup if DHCP is required for your configuration.
- If you start and then end the autoinstall program before the DHCP server replies, DHCP requests are ignored. The workaround is to wait until you see the IP address appear when it is provided by the DCHP server.
- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted up without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

1. Disable auto-QoS on the interface.
2. Change the routed port to a nonrouted port or the reverse.
3. Re-enable auto-QoS on the interface. (CSCec44169)

- The DHCP snooping binding database is not written to flash or a remote file in either of these situations:
  - The DHCP snooping database file is manually removed from the file system. After you enable the DHCP snooping database by configuring a database URL, a database file is created. If you manually remove the file from the system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - The URL for the configured DHCP snooping database was replaced because the original URL is not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)
- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)
- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)
- A traceback error occurs if a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

Ethernet

Subnetwork Access Protocol (SNAP) encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)

HSRP

When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list. The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

IP

When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

IP Telephony

These are the IP telephony limitations:

- After you change the access VLAN on a port that has 802.1x enabled, the IP Phone address is removed. Because learning is restricted on 802.1x capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)

Multicasting

These are the multicasting limitations:

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- If an IG MP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)

QoS

These are the quality of service (QoS) limitations:

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the replicate option. For a remote SPAN session, there is no workaround.

  This is a hardware limitation: (CSCdy72835)

- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the encapsulation replicate option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround.

  This is a hardware limitation: (CSCdy81521)

- During periods of very high traffic, when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session.

  This is a hardware limitation: (CSCed24036)

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN.

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the LED to blink amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an 802.1Q trunk interface. There is no workaround. (CSCdz33708)

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909)

- For trunk ports or access ports configured with 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100)

VLAN

If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail. The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

Device Manager Limitations and Restrictions

These are the device manager limitations and restrictions:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI.
- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Hardware Limitations and Restrictions

These are the hardware limitations and restrictions:

When using CLC-T SFPs in CGESM switches, the SFP module can be installed too far into the switch. This can prevent links from operating properly.

The workaround is to slightly pull the SFP out of the module slot. (CSCsd17765)

Device Manager Notes

These notes apply to the device manager:

- We recommend that you use this browser setting to display the device manager from Microsoft Internet Explorer in the least amount of time.

  From Microsoft Internet Explorer:

  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the "Temporary Internet files" area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

  Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.

VLAN Interfaces and MAC Addresses

All VLAN interfaces have assigned MAC addresses that are derived from the base MAC address. The base MAC address is the hardware address that is on the switch label. It also appears when you enter the **show version** privileged EXEC command.

On the first VLAN interface (VLAN 1), the MAC address is the base MAC address + 0 x 40. On the next VLAN interface that you configure, the MAC address is the base MAC address + 0 x 40 +1, and so on for other VLAN interfaces.

You can enter the **show interfaces vlan vlan-id** privileged EXEC command to show the MAC and IP addresses. The MAC addresses that appear in the **show interfaces vlan vlan-id** command output are not the same as the MAC address that is printed on the switch label (the base MAC address).

By default, VLAN 1 is the interface that connects to the management network. When the switch boots up, the DHCP client (switch) requests an IP address from a DHCP server by using the MAC address of VLAN 1.

Documentation Notes

This section describes documentation notes related to this IOS release.

References to IOS Release Number

These documents refer to Release 12.2(25)SE. The correct release is Release 12.2(25)SE1.

- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Software Configuration Guide, Cisco IOS Release 12.2(25)SE*
- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Command Reference Guide, Cisco IOS Release 12.2(25)SE*
- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class System Message Guide, Cisco IOS Release 12.2(25)SE*

Open Caveats

These sections describe the open caveats with possible unexpected activity in this software release:

- "Open IOS Caveats" section on page 14
- "Open Device Manager Caveats" section on page 17

Open IOS Caveats

These severity 3 Cisco IOS configuration caveats apply to the CGESM switch:

- CSCee08109

  If a port-based ACL (PACL) is applied to an 802.1x-enabled port and the client is then disconnected from that port, the PACL is not removed from the port.

  There is no workaround.

- CSCeg04311

  When you power on or restart a switch that does not have a config.text file in flash memory, the switch tries to get configuration files from a TFTP server. If the configuration files are not found, the switch automatically configures the **service config** global configuration command, which causes the switch to continue searching (in the background) for the expected configuration files.

  If the **service config** command does not find the configuration files, these error messages appear:

  ```
  %Error opening tftp://255.255.255.255/network-confg (Timed out)
  %Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
  %Error opening tftp://255.255.255.255/router-confg (Timed out)
  %Error opening tftp://255.255.255.255/ciscortr.cfg (Timed out)
  ```

  These system messages also appear:

  ```
  00:01:40: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from
  (tftp://255.255.255.255/network-confg) failed
   00:01:40: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from
  (tftp://255.255.255.255/cisconet.cfg) failed
   00:01:40: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from
  (tftp://255.255.255.255/switch-confg) failed
   00:01:40: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from
  (tftp://255.255.255.255/ciscortr.cfg) failed
  ```

  These messages are for information only. There is no problem with the switch operation.

  Because the switch automatically configures the **service config** global configuration command, it is in the switch startup-config file when you save the running-config file. This command runs every time the switch is restarted, even if a config.text configuration file is in the switch flash memory.

  The workaround is to prevent these messages from being generated. To do this, enter the switch configuration mode, and issue the **no service config** command. Save the configuration to flash by using the **copy running-config to startup-config** command. The preceding error and system messages no longer appear and do not appear when the switch is restarted.

- CSCeg67844

  When using SNMP, the CGESM switch returns an incorrect value of 65534 for the ciscoFlashPartitionFileCount MIB; the switch actually contains 1367 files.

  There is no workaround.

- CSCsb85001

  If traffic is passing through VMPS ports and you perform a **shut** operation, a dynamic VLAN is not assigned and a VLAN with a null ID appears.

  The workaround is to clear the MAC address table. This forces the VMPS server to correctly reassign the VLAN.

- CSCsc26726

  Sometimes interfaces Gi0/23 & Gi0/24 will not link up with another switch when the interface speed is set to an explicit value instead of autonegotiated. This does not happen when a copper SFP is used with interfaces Gi0/17 - Gi0/20.

  The workaround is to autonegotiate the speed with the other device, or to use a different cable type. Use a straight through cable for switch to switch connection, or a cross-over cable for switch to any non switch device connection. If the other device is capable of auto MDIX even with speed not set to auto, then use that. When an improper cable is used only one side of the connection needs to use auto MDIX to achieve a link.

- CSCsd78044

  When IGMP snooping is enabled and an EtherChannel member interface goes down, the switch might stop forwarding multicast traffic on the EtherChannel. This problem occurs when the EtherChannel interface is a member of a multicast group that is not directly connected (that is, the multicast group that does not have the *C* flag set in the **show ip mroute** privileged EXEC command output).

  The workaround is to either disable IGMP snooping, or to use the **clear ip mroute** user EXEC command to refresh all the routes.

- CSCsd85770

  When you apply the **mls qos trust dscp** global configuration command to a port, this error message might appear.

  ```
  Master sets trust failed, sets to untrust modetrust type update
  failed on ifc GigabitEthernetx/x
  Switch(config-if)#Tcam write failed trust dscp
  %QOSMGR-4-COMMAND_FAILURE: Execution of slave:HQM_IDBTRUST_CMD
  command failed on GigabitEthernetx/x
  ```

  The workaround is to apply the **sdm prefer qos** global configuration command before you enter the **mls qos trust dscp** global configuration command.

- CSCsd86177

  When you remove and reconfigure a loopback interface, it does not appear in the ifTable.

  The workaround is to reload the switch.

- CSCse03859

  If the switch is in VTP server mode and VLANs with IDs greater than 255 (256 and above) are created, DHCP snooping does not work properly on these VLANs.

  The workaround is to put the switch in VTP transparent mode before creating the VLANs.

- CSCse06827

  When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state.

  The workaround is to configure the burst interval to more than 1 second.

- CSCse14774

  If a switch is connected to a third-party router through an EtherChannel and the EtherChannel is running in Link Aggregation Control Protocol (LACP) mode, the interfaces in the EtherChannel might go down after you enter the **switchport trunk native vlan** *vlan-id* interface configuration command to change the native VLAN from VLAN 1 (the default) to a different VLAN ID.

  These are the workarounds. You only need to do one of these:

  - Do not change the native VLAN ID from the default setting of VLAN 1.
  - If you need to change the native VLAN ID to a VLAN other than VLAN 1, do not run the EtherChannel in LACP mode, and change the mode to *On* by using the **channel-group** *channel-group-number* **mode on** interface configuration command.

- CSCsg21537

  When MAC addresses are learned on an Etherchannel port, the addresses are incorrectly deleted from the MAC address table even when the MAC address table aging timeout value is configured to be longer than the ARP timeout value. This causes intermittent unicast packet flooding in the network.

  The MAC address is automatically relearned after the ARP refresh. The workaround is to enter the **ping** *ip address* privileged EXEC command from the switch to the next hop router to avoid the intermittent flooding.

- CSCsg79506

  During repeated reauthentication of supplicants on an IEEE 802.1x-enabled switch, if the RADIUS server is repeatedly going out of service and then coming back up, the available switch memory might deplete over time, eventually causing the switch to shut down.

  There is no work-around, except to ensure that the RADIUS server is stable.

- CSCsg81334

  If IEEE 802.1x critical authentication is not enabled and the RADIUS authentication server is temporarily unavailable during a reauthentication, when the RADIUS server comes back up, MAC authentication bypass (MAB) does not authenticate a previously authenticated client.

  The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command on the port connected to the client. An alternative, to prevent the problem from occurring, is to enable critical authentication by entering the **dot1x critical** {**eapol** | **recovery delay** *milliseconds*} global configuration command.

- CSCsi63999

  Changing the spanning tree mode from rapid STP to MSTP can cause tracebacks when the virtual port error-disable feature is enabled when the STP mode is changed.

  There is no workaround.

- CSCsi75246

  An address learned as a supplicant that is aged out by port security aging is never relearned by port security under any of these conditions:

  - IEEE 802.1x authentication, port security, and port security aging are enabled on a port.
  - An address is cleared by port security.
  - You enter the **clear port security** privileged EXEC command.

  The workaround is to use the **dot1x timeout** interface configuration command instead of the port security aging timer as the reauthentication timer for IEEE 802.

Open HP Caveats

These are the HP severity 2 open caveats for this release:

- rQm 263546

  Disconnecting the cable from the console port does not end a Telnet session. If you are in privileged EXEC mode when you remove the cable, the next session that is started on the console port will also be in privileged EXEC mode.

  The workaround is to end the session before you remove the cable.

- rQm 266129

  If you power on a switch that does not have a config.txt file (the factory default file) and leave the switch on for few hours, the switch console appears to be stalled during setup.

  The workaround is to reload the switch before you continue to configure it.

Open Device Manager Caveats

This is the severity 3 device manager caveat for this release:

- CSCef94061

  If you enter the letter *i* by itself in the port description, the VLAN status column displays *i*; this only occurs when you are using Device Manager through Netscape 7.1.

  The workaround is to run Device Manager through Internet Explorer if you must enter a port description with only the value “i.”

Resolved Caveats

These sections describe the caveats that have been resolved in these releases:

- Caveats Resolved in Cisco IOS Release 12.2(37)SE1, page 17
- Caveats Resolved in Cisco IOS Release 12.2(37)SE, page 18

Caveats Resolved in Cisco IOS Release 12.2(37)SE1

These caveats are resolved in Cisco IOS Release 12.2.(37)SE1:

- CSCsc19259

  The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device’s filesystem, including the device’s saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- CSCsj13619

  The SCP (Secure Copy Protocol) support is now correctly included in the image. The **show file systems** and **copy** privileged EXEC commands now correctly show **scp** as an option.

- CSCsj19641

  The switch no longer drops ARP packets destined to MAC addresses that are close to the MAC address block of the switch.

Caveats Resolved in Cisco IOS Release 12.2(37)SE

These caveats are resolved in Cisco IOS Release 12.2.(37)SE:

- CSCsb12598

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsb40304

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  – Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

  – Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

  – Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsc30733

  This error message no longer appears during authentication when a method list is used and one of the methods in the method list is removed:

  ```
  AAA-3-BADMETHODERROR:Cannot process authentication method 218959117
  ```

- CSCsd60718

  When you enter the **no speed** interface configuration command, the Ethernet interface speed now correctly returns to its default setting. This affects interfaces Gigabit Ethernet 0/17 to Gigabit Ethernet 0/20, Gigabit Ethernet 0/23, and Gigabit Ethernet 0/24. This does not affect interfaces Gigabit Ethernet 0/21 and Gigabit Ethernet 0/22.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsg18176

  When dynamic ARP inspection is enabled and IP validation is disabled, the switch no longer drops ARP requests that have a source address of 0.0.0.0.

- CSCsg30295

  When you configure an IP address on a switch virtual interface (SVI) with DCHP and enable DHCP snooping on the SVI VLAN, the switch SVI now obtains an IP address.

- CSCsh92834

  When trunk ports are participating in a Flex Link configuration, entering a **shutdown** or **no shutdown** interface configuration command on the port no longer causes the switch to reload.

- CSCsh92844

  Online insertion and removal (OIR) of an SFP module no longer causes error-disabled ports to change to Up or Standby states, resulting in lost data.

- CSCsi00879

  When IGMP snooping is enabled, multicast traffic no longer is dropped after a port channel interface link flaps.

- CSCsi30888

  The switch no longer halts when configuring link-state tracking with EtherChannel downstream ports or when booting up a switch already configured with link-state tracking with EtherChannel downstream ports.

Updates to the Software Configuration Guide

This section was added to the "Configuring IEEE 802.1x" chapter:

Web Authentication with Automatic MAC Check

You can use web authentication with automatic MAC check to authenticate a client that does not support IEEE 802.1x or web browser functionality. This allows end hosts, such as printers, to automatically authenticate by using the MAC address without any additional required configuration.

Web authentication with automatic MAC check only works in web authentication standalone mode. You cannot use this if web authentication is configured as a fallback to IEEE 802.1x authentication.

The MAC address of the device must be configured in the Access Control Server (ACS) for the automatic MAC check to succeed. The automatic MAC check allows managed devices, such as printers, to skip web authentication.

Note The interoperability of web authentication (with automatic MAC check) and IEEE 802.1x MAC authentication configured on different ports of the same switch is not supported.

Related Documentation

These documents provide complete information about the switch and are available from the HP web site:

http://www.hp.com/support

- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Release Notes* (part number 383623-001)
- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Software Configuration Guide* (part number 380261-001)
- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class System Message Guide* (part number 380260-001)
- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Hardware Installation Guide* (part number 380264-001)
- *Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Quick Setup Instructions* (part number 380263-001)
- *Cisco Small Form-Factor Pluggable Modules Installation Instructions* (part number 380-263-001)
- *HP BladeSystem p-Class SAN Connectivity Kit Quick Setup Instructions For Installing in Cisco Gigabit Ethernet Switch Module* (part number 380262-001)

Cisco IOS Release 12.2 documentation is available at

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/index.html

Technical support

These sections provide information about how to find technical support.

Before you contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Product identification number
- Applicable error messages
- Add-on boards or hardware

- Third-party hardware or software
- Operating system type and revision level

HP contact information

For the name of the nearest HP authorized reseller:

- In the United States, see the HP US service locator webpage (http://www.hp.com/service_locator).
- In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (http://www.hp.com).
- In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).