

Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Release Notes, Cisco IOS Release 12.2(52)SE

October 1, 2009

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:

- “[System Requirements](#)” section on page 2
- “[Upgrading the Switch Software](#)” section on page 3
- “[Installation Notes](#)” section on page 5
- “[New Software Features](#)” section on page 5
- “[Minimum Cisco IOS Release for Major Features](#)” section on page 5
- “[Limitations and Restrictions](#)” section on page 6
- “[Device Manager Notes](#)” section on page 11
- “[VLAN Interfaces and MAC Addresses](#)” section on page 12
- “[Open Caveats](#)” section on page 13
- “[Resolved Caveats](#)” section on page 14
- “[Documentation Updates](#)” section on page 15



- [“Related Documentation” section on page 15](#)
- [“Technical support” section on page 16](#)

System Requirements

The system requirements are described in these sections:

- [“Device Manager System Requirements” section on page 2](#)
- [“Cluster Compatibility” section on page 2](#)

Device Manager System Requirements

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

- [“Hardware Requirements” section on page 2](#)
- [“Software Requirements” section on page 2](#)

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

These are the supported operating systems and browsers for the device manager:

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 5.5, 6.0, 7.0, Firefox 1.5, 2.0 or later.

The device manager verifies the browser version when starting a session, and it does not require a plug-in.

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 3
- “[Upgrading a Switch by Using the Device Manager](#)” section on page 3
- “[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.122-52.SE.tar
- cgesm-lanbasek9-tar.122-52.SE.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

There are no new software features for this release.

Minimum Cisco IOS Release for Major Features

[Table 2](#) lists the minimum software release required to support the major features on this switch.

Table 2 CGESM Switch Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
Generic message authentication support with the SSH Protocol and compliance with RFC 4256.	12.2(46)SE
IPv6 default router preference (DRP)	12.2(46)SE
DHCP server port-based address allocation	12.2(46)SE
Configuration replacement and rollback	12.2(40)SE
IP Service Level Agreements (IP SLAs) responder	12.2(40)SE
Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE
Support for the CISCO-MAC-NOTIFICATION-MIB	12.2(40)SE
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

Table 2 CGESM Switch Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
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” section on page 6](#)
- [“Device Manager Limitations and Restrictions” section on page 10](#)
- [“Hardware Limitations and Restrictions” section on page 11](#)

Cisco IOS Limitations

These limitations apply to CGESM switch:

- [“Configuration” section on page 7](#)
- [“Ethernet” section on page 8](#)
- [“HSRP” section on page 8](#)
- [“IP” section on page 8](#)
- [“IP Telephony” section on page 8](#)
- [“Multicasting” section on page 8](#)
- [“QoS” section on page 9](#)
- [“SPAN and RSPAN” section on page 9](#)
- [“Trunking” section on page 10](#)

- [“VLAN” section on page 10](#)

Configuration

These are the configuration limitations:

- If you run the CLI-based setup program, the IP address that the Dynamic Host Configuration Protocol (DHCP) 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 DHCP 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. (CSCe71176 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)
- When system jumbo MTU size is configured on a switch and the egress ports can support jumbo frames, the egress SPAN jumbo frames are not forwarded to the SPAN destination ports.
There is no workaround. (CSCsj21718)

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

This is the IP telephony limitation:

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 IGMP 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

These are the VLAN limitations:

- 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)
- 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. (CSCse06827)

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

This is the hardware limitation and restriction:

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)

Important Notes

These sections describe the important notes related to this software release:

- [“Cisco IOS Notes” section on page 11](#)
- [“Device Manager Notes” section on page 11](#)

Cisco IOS Notes

These notes apply to Cisco IOS software:

- Cisco IOS Release 12.2(40)SE and later

If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software to Cisco IOS Release 12.2(40)SE (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

```
AutoQoS Error: ciscophone input service policy was not properly applied
policy map AutoQoS-Police-CiscoPhone not configured
```

If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

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.

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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {aaa enable local}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> • aaa—Enable the authentication, authorization, and accounting feature. You must enter the aaa new-model interface configuration command for the aaa keyword to appear. • 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.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	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 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 Cisco IOS Release 12.2(25)SE

These older 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

Open IOS Caveats

These severity Cisco IOS configuration caveat applies to the CGESM switch:

- CSCsz18634
On a switch running Cisco IOS release 12.2(46)SE, the output of the **show interfaces** privileged EXEC command shows 0 packets for port channel input and output rates.
The workaround is to reload the switch by entering the **reload** privileged EXEC command.
- CSCtc02635
On switches running Cisco IOS release 12.2(50)SE3 running MAC authentication bypass with multidomain authentication (MDA, IP phones connected to a port might not be able to regain network connectivity in the VOICE domain if the session times out and all RADIUS servers are unreachable.
There is no workaround.

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.

Resolved Caveats

- CSCsw68528

When you use the **show mvr interface interface members** privileged EXEC command to view the Multicast VLAN Registration (MVR) interface group status, the switch incorrectly displays the status ACTIVE for port members that are not connected.

The workaround is to use the **show mvr interface interface** or **show mvr members** privileged EXEC command to display the port MVR status.

- CSCsx71632

When VLAN-based quality of service (QoS) is enabled and then disabled on an interface by entering the **mls qos vlan-based** interface configuration command followed by the **no** version of the command, the port policy is not applied properly and could result in undefined behavior for packets matching the port policy.

The workaround is to remove the port policy by entering the **no service-policy input policy-map-name** interface configuration command and then reapply it to the interface.

- CSCsx78068

If you enable 802.1Q native VLAN tagging by entering the **vlan dot1q tag native** global configuration command and then change the native VLAN ID on an ingress trunk port by entering the **switchport trunk native vlan vlan-id** interface command, untagged traffic is forwarded instead of being dropped.

The workaround is to use one of these methods:

- Enter a **shutdown** followed by a **no shutdown** interface configuration command on the trunk port.
- Disable and then reenables native VLAN tagging by entering the **no vlan dot1q tag native** global configuration command followed by the **vlan dot1q tag native** command.

- CSCsy90265

If you repeatedly enter the **show tech-support** privileged EXEC command, the switch might leak memory and, in some cases, shut down.

The workaround is to reload the switch to clear the memory after repeated use of the **show tech-support** command.

- CSCta57846

The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

The workaround is to enter the **logging file flash:filename** global configuration command to configure logging to flash instead of copying to flash.

- CSCta78502
When you have configured a login banner by entering the **banner login c message c** global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.
There is no workaround.
- CSCtb97439
When remote neighbors change, the LLDP MIB does not properly update the remote neighbors.
The workaround is to clear the LLDP table by entering the **clear lldp table** privileged EXEC command.

Documentation Updates

Update to the Software Configuration Guide

This text was updated in the “Using IEEE 802.1x Authentication with Guest VLAN” section of the software configuration guide:

If the switch is trying to authorize an IEEE 802.1x-capable voice device and the AAA server is unavailable, the authorization attempt fails, but the detection of the EAPOL packet is saved in the EAPOL history. When the AAA server becomes available, the switch authorizes the voice device. However, the switch no longer allows other devices access to the guest VLAN. To prevent this situation, use one of these command sequences:

- Enter the **dot1x guest-vlan supplicant** global configuration command to allow access to the guest VLAN.
- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to restart the port.

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

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
- 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>).