

# Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Release Notes, Cisco IOS Release 12.2(25)SEE1 and later

---

Revised June 10, 2008

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.



**Note**

---

The documentation for the CGESM switch refers to IOS Release 12.2(25)SE. For a complete list of these documents, see the [“Documentation Notes” section on page 13](#).

This document provides updates to Cisco IOS Release 12.2(25)SEE1 and Cisco IOS Release 12.2(25)SEE2

---

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](#)
- [“Major Features” section on page 6](#)
- [“Minimum Cisco IOS Release for Major Features” section on page 6](#)
- [“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 16
- “Related Documentation” section on page 21
- “Technical support” section on page 21

## System Requirements

The system requirements are described in these sections:

- “Device Manager System Requirements” section on page 2
- “Cluster Compatibility” section on page 3

## 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 <sup>1</sup>	64 MB <sup>2</sup>	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 <sup>1</sup>	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.122-25.SEE4.tar
- cgesm-lanbasek9-tar.122-25.SEE2.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*.

## Major Features

This release contains no new features.

## 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
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 11](#)
- [“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 9
- “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 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 Mbps full duplex or 100 Mbps 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 Mbps 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 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

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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication { enable   local   tacacs }</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> <li>• <b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li>• <b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> <li>• <b>tacacs</b>—TACACS server is used.</li> </ul>

	Command	Purpose
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. <ul style="list-style-type: none"> <li><b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li><b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> <li><b>tacacs</b>—TACACS server is used.</li> </ul>
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 13](#)
- [“Open Device Manager Caveats” section on page 16](#)

## 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 PAACL is not removed from the port.  
There is no workaround.
- CSCee22376  
When an SNMP version 3 user is configured with the encrypted option and password, the switch reloads when the MIB object `usmUserAuthKeyChange` is set.  
The workaround is to configure a user without the encrypted option. (For example, **`snmp-server user username groupname v3 auth md5 password.`**)
- 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-config (Timed out)
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
%Error opening tftp://255.255.255.255/router-config (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-config) 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-config) 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.

- CSCsd49367

When a switch is running DHCP option 82 and is connected to several other switches by Gigastack GBICS, a PC connecting to that switch might fail to obtain an IP address. This connection attempt can fail several times. Eventually, the PC might connect to the switch.

This is an intermittent problem. There is no workaround.

- 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.

- 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.

- 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.

## 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 resolved caveats for the CGESM switch:

- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)SEE4” section on page 16](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)SEE2” section on page 17](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)SEE1” section on page 18](#)
- [“Resolved Device Manager Caveat” section on page 20](#)

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)SEE4

These are the resolved IOS caveats in Cisco IOS Release 12.2(25)SEE4:

- CSCsf04754  
Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

- CSCsh89429

The switch no longer reloads when the **write core** privileged EXEC command is entered when testing a core dump configuration and FTP is selected as the file transfer protocol.

- CSCsj39211

The switch no longer incorrectly overwrites the class of service (CoS) packets of internally generated Multicast Listener Discovery (MLD) queries and other control packets.

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)SEE2

These are the resolved IOS caveats in Cisco IOS Release 12.2(25)SEE1:

- CSCec71950

Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing. This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

- CSCef73145

The Mean Opinion Score (MOS) reported by an IP SLA jitter probe is now correct.

- CSCek26492

Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

- CSCsb81283

MAC notifications now work properly when port security is configured.

- CSCsd51530

When you telnet to a switch and enter the **autocommand-options nohangup** interface configuration command on VTY lines 0 through 4, you can now successfully log out and telnet back into the switch.

In previous releases, when you logged out of the switch and then tried to open a new Telnet session, the switch would automatically log you out.

- CSCse48664

The dot1dBasePort values in the Bridge-MIB now match the front-panel numbering for the switch FastEthernet interfaces.

- CSCse49694

These error messages no longer appear on a CGESM switch running Cisco IOS Release 12.2(25)SEE2 or later:

```
00:01:32: %PLATFORM_ENV-1-PWR: Faulty redundant power supply detected
00:01:31: %PLATFORM_ENV-1-PWR: Faulty internal power supply detected
```

In previous releases, the messages appeared when the image was first loaded onto the switch and continued to appear every five minutes.

- CSCse55723

A Telnet session no longer stops if you press the Space or Enter key when the show command output is scrolling.

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)SEE1

These are the resolved IOS caveats in Cisco IOS Release 12.2(25)SEE1:

- CSCea80105

When a Cisco IP Phone is connected to a switch, only the Voice VLAN (VVID) of the switch learns the MAC address of phone. This is the correct behavior.

In previous releases, the MAC address was learned on both the VVID and the Data VLAN (PVID). When the dynamic MAC addresses were removed (manually or automatically) either by a topology change or by enabling or disabling the port security or IEEE 802.1x feature, the MAC address of Cisco IP Phones MAC address was re-learned only on the VVID.

- CSCee37070

When an 802.1x-enabled port is in single-host mode and has port security enabled, the port no longer goes into the error-disabled state and displays this system message if another MAC address is detected on the port:

```
%DOT1X-SECURITY_VIOLATION
```

- CSCef65587

These error messages no longer randomly appear:

```
%SYS-2-NOBLOCK: idle with blocking disabled. -Process= "hpm main process", ipl= 0,
pid= 62
-Traceback= 259CC0 251438 750244 661220 665774 6603CC 653750 6575B0 64FC44 651260
65DF58 4EC268 544300 4F5F64 4B433C 522508
*Sep 2 15:42:22: %SYS-2-BLOCKHUNG: Task hung with blocking disabled, value = 0x1.
-Process= "hpm main process", ipl= 0, pid= 62
-Traceback= 259CFC 251438 750244 661220 665774 6603CC 653750 6575B0 64FC44 651260
65DF58 4EC268 544300 4F5F64 4B433C 522508
```

- CSCei80087  
It is no longer necessary to detach and then reapply a hierarchical policy map to force changes to a VLAN level class-map to take effect.
- CSCek26492  
Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:  
<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>  
Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.  
Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:  
<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>
- CSCek37177  
The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.  
This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.  
Cisco has made free software available to address this vulnerability for affected customers.  
This issue is documented as Cisco bug ID [CSCek37177](#).  
There are workarounds available to mitigate the effects of the vulnerability.  
This advisory is posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>
- CSCsb79198  
A switch no longer fails IEEE 802.1x authentication if it downloads an access control list (ACL) that has more than 20 ACL access control entries (ACEs) from a RADIUS server.
- CSCsb82422  
The switch now forwards an IEEE 802.1x request that has *null* credentials.
- CSCsc13467  
A switch no longer fails or displays illegal memory access messages during the SNMP Timer process.
- CSCsc58665  
The ENTITY-MIB: entPhysicalVendorType now returns correct information for SFP ports.
- CSCsc81978  
When the switch displays a `STORM_CONTROL-3-SHUTDOWN` message and a port status changes to disabled, the `cpscEvent (cpscStatus) Trap` now correctly shows that the `CPortStormControlStatusType` is 5, which means *shutdown*.  
In previous releases, the trap showed 2, which means *forwarding*.
- CSCsc84627  
A MAC entry no longer changes from *static* to *dynamic* on a switch configured with Private VLANs.

- CSCsc84880  
When the **radius-server source-ports 1645-1646** global configuration command is removed, the switch no longer sends the RADIUS server requests with incorrect source ports.
- CSCsd16059  
A switch now correctly forwards nonstandard Virtual Router Redundancy Protocol (VRRP) packets. (In nonstandard VRRP packets, the Layer 3 destination is a multicast address, but the Layer 2 destination address is a unicast address.)
- CSCsd16908  
If the **dot1x port-control auto/force-unauthorized** interface configuration command has been entered while IEEE 802.1x is globally disabled, it is no longer necessary to enter the **no dot1x port-control** interface configuration command to return to the default setting of **force-authorized**.
- CSCsd19470  
This error log message no longer randomly appears:  

```
%TCAMMGR-3-HANDLE_ERROR: cam handle [hex] is invalid
```
- CSCsd24183  
A switch no longer fails when a user logs in, the **debug radius** privileged EXEC command is enabled, and the RADIUS server is sending an unsupported attribute value.
- CSCsd30129  
After you delete a global- or interface-level NAC Layer 2 IP configuration by using the **no ip admission name global- or interface-configuration** command, the switch no longer fails and displays a message similar to this:  

```
Unexpected exception to CPUvector 700, PC = 3CEDAC0  
-Traceback= 3CEDAC0 45106C C82010 C3D4F4 C3D618 C40B94 FE7EA0 2BBA34 2B28B8 AE8BEC  
B035CC 8F3F84 8EA54C
```
- CSCsd79916  
An authenticated IEEE 802.1X port now passes traffic to an attached PC if the switch port is configured with a voice VLAN, the attached PC is configured to perform both machine and user authentication, and the machine and user authentication on the PC the result in different VLANs being assigned to the port.
- CSCsd81205  
When a supplicant authenticates, the switch no longer fails if a value for *attribute 11* is configured on the RADIUS server.

## Resolved Device Manager Caveat

This is the resolved device manager caveat:

- CSCef78853  
Entering certain characters in some menu items in the device manager window can cause the front panel of a switch to not appear or error dialogs to appear. This can occur when a semicolon (;), single quotation mark ('), or double quotation mark (") is used as part of the hostname, port description, SNMP system location, SNMP system contact, SNMP community strings, Telnet password, or switch password.  
The workaround is to remove the character from names of these menu items.

## 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
- 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](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](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>).