Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem

Release Notes, Cisco IOS Release 12.2(25)SED

Part number: 405534-001

First edition: November 2005

November 2005

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

NOTE: The documentation for the CGESM switch refers to Cisco IOS Release 12.2(25)SE. The correct Cisco IOS release is Cisco IOS Release 12.2(25)SED. For a complete list of these documents, see the Documentation notes section.

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).

You can download the switch software from this URL:

http://www.hp.com/support

Contents

This information is in the release notes:

System requirements

The system requirements are described in the Device manager system requirements section.

Device manager system requirements

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

- Hardware requirements
- Software requirements

Hardware requirements

The following table 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

The following table 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 98	None	5.5 or 6.0	7.1
Windows NT	Service Pack 6 or later	5.5 or 6.0	7.1
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.

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
- Deciding which files to use
- Archiving software images
- Upgrading a switch by using the device manager
- Upgrading a switch by using the CLI
- Recovering from a software failure

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-lanbasek9-tar.122-25.SED.tar
- cgesm-lanbase-tar.122-25.SED.tar

Archiving software images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

HP routinely removes old Cisco IOS versions from http://www.hp.com. You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the `copy flash: tftp:` privileged EXEC command.

NOTE: Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from http://www.hp.com/support and archive it on an internal host in your network.

Upgrading a switch by using the device manager

You can upgrade switch software by using the device manager. From the feature bar, choose 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 software, follow these steps:

1. To download the software image file go to http://www.hp.com/support.

   Select the appropriate region, and then search on `CGESM` with the Download drivers and software radio button selected.

   To download the image for a CGESM switch, click on the desired blade infrastructure or firmware release. You may obtain authorization and download the cryptographic software files by clicking on the software depot link in the note section and searching on `CGESM` in the software depot.
2. Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

   For more information, see Appendix B in the *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Software Configuration Guide* for this release.
3. Log into the switch through the console port or a Telnet session.
4. (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, see the software configuration guide for this release.
5. 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-lanbase-
   tar.122-25.SED.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 p-Class BladeSystem 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 p-Class BladeSystem Hardware Installation Guide*.
- The CLI-based setup program, as described in the *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Hardware Installation Guide*.
- The DHCP-based autoconfiguration, as described in the *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Software Configuration Guide*.
- Manually assigning an IP address, as described in the *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Software Configuration Guide*.

Major features

This release contains these features:

- The device manager is included in the switch image and provides simplified management for a single switch. Its features, such as Smartports and color-coded graphs, make it easier to configure and monitor the switch. No special installation is required. After the switch is configured through the Express Setup program or through the CLI-based setup program, the device manager is accessible through a Microsoft Internet Explorer or Netscape Navigator browser session. For more information, see the device manager online help. For information on how to display the device manager, see the *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Hardware Installation Guide*.
- Secure Socket Layer (SSL) version 3.0 support for the HTTP1.1 server authentication, encryption, and message integrity, and HTTP client authentication to allow secure HTTP communications (only available in the cryptographic software image)
- Storm-control enhancements:
  - Specify the traffic rate in packets per second or in bits per second at which broadcast, multicast, or unicast packets are received.
  - Specify an action to take when a storm control occurs on a port.
- Support for DSCP transparency. If DSCP transparency is enabled, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.
- Support for VLAN-based QoS and hierarchical policy maps on switch virtual interfaces (SVIs).
- IP IGMP snooping querier to determine if any devices connected to a switch interface are interested in traffic for a specific multicast group.
- IGMP leave timer to configure the leave latency for the network.
- Support for frame sizes up to 9216 bytes.
- Layer 2 trunk failover, also known as link-state tracking, for Layer 2 redundancy in the network.
- EtherChannel load balancing based on source IP and destination IP addresses.
- Port blocking on forwarding unknown unicast and multicast traffic.
- Beginning with this release, Cluster Management Suite (CMS) is no longer available with the switch software. You can use the embedded device manager to configure or to manage a single switch.

  The device manager is included in the switch image and provides simplified management for a single switch. No special installation is required. The device manager is accessible through a Microsoft Internet Explorer or a Netscape Navigator browser session. For more information, see the device manager online help.
- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files. Catalyst 3750 and 3560 switches and Cisco EtherSwitch service modules require the cryptographic versions of the software IP base and IP services images, and Catalyst 2970 and CGESM switches require the cryptographic version of the software.
- Configuration logging to log and to view changes to the switch configuration.
- Unique device identifier to provide product identification information through a `show inventory` user EXEC command display.
- Support for multiple spanning-tree (MST) based on the IEEE 802.1s standard.
- IEEE 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame.

Minimum Cisco IOS release for major features

The following table 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
Trunk failover (Layer 2 trunk failover or link state tracking)	12.2(25)SE2
Configurable IGMP leave timer	12.2(25)SED

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
- Device manager limitations and restrictions

Cisco IOS limitations

These limitations apply to CGESM switch:

- Configuration
- Ethernet
- HSRP
- IP
- IP telephony
- Multicasting
- QoS
- SPAN and RSPAN
- Trunking
- VLAN

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. (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 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)
- 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 *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem 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:

- When a Cisco IP Phone is connected to the switch, the port VLAN ID (PVID) and the voice VLAN ID (VVID) both learn its MAC address. However, after dynamic MAC addresses are deleted, only the VVID relearns the phone MAC address. MAC addresses are manually or automatically deleted when a topology change occurs or when port security or an 802.1x feature is enabled or disabled. There is no workaround. (CSCea80105)
- 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

You cannot create and manage switch clusters through the device manager.

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. Select Tools > Internet Options.
  2. Click Settings in the “Temporary Internet files” area.
  3. From the Settings window, select 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 Cisco IOS release.

References to Cisco IOS release number

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

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

Open Cisco IOS caveats

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

- CSCee12496

  When a switch is in interface range configuration mode and you enter the `ip arp inspection trust` command to set a range of ports to trusted mode, if some of those ports are members of a channel-group this error message might appear:

  ```
  %PM-3-INTERNALERROR: Port Manager Internal Software Error (pd->physicalPort
  && pd->agPort == NULL: ../switch/pm/pm_port.c: 3865: pm_port_want_to_bundle)
  ```

  There is no workaround.
- CSCee22376

  When a switch using SNMP version 3 is configured with the encrypted option and password, the switch reloads when the MIB object usmUserAuthKeyChange is set.

  The workaround is to configure the switch without the encrypted option. (For example, `snmp-server user username groupname v3 auth md5 password`.)
- CSCee93822

  When port security is enabled on an interface in restricted mode and the `switchport block unicast` interface command is entered for 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 for that specific interface.
- CSCeg04311

  When you power on or restart a switch without 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, and the switch continues to search 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.

- CSCeg09032

  Open Shortest Path First (OSPF) routes might not appear in the routing table after a topology change if incremental SPF (iSPF) is enabled.

  The workaround is to disable iSPF.

- 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.

- CSCsb79318

  If the re-authentication timer and re-authentication action is downloaded from the RADIUS server using the Session-Timeout and Termination-Action RADIUS attributes, the switch performs the termination action even when the port is not configured with the `dot1x timeout reauth server` global configuration command and uses the Termination-Action downloaded from a RADIUS server as part of IEEE 802.1x authorization.

  The workaround is to remove the Termination-Action attribute from the IEEE 802.1x policy on the RADIUS server if dot1x timeout reauth server is not configured on the port.

- CSCsb82422

  The switch does not forward an IEEE802.1x request that has null credentials.

  There is no workaround.

- CSCsb82459

  When a supplicant is IEEE 802.1x-capable and also performs DHCP, the switch might send an interim update before DHCP is complete but after an EAP-Success message is sent. When this happens, the interim update might be inaccurate.

  There is no workaround.

- CSCsb85552

  Enabling link state groups on downstream interfaces before an upstream interface is configured causes downstream ports to go down.

  The workaround is to configure the upstream interfaces into the link state group first. Then configure the downstream interfaces. The downstream interfaces should recover and be allowed to go link up by the link state tracking process.

- 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

These are the severity 3 device manager caveats for this release:

- CSCef45718

  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.
- 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 caveats were resolved in this release for the CGESM switch:

- CSCed23767

  The `switchport port-security aging time 0` interface configuration command now disables the aging time.
- CSCed37222

  Sticky addresses are no longer lost during a master switchover.
- CSCed46781

  When you configured the `dot1x timeout tx-period` interface configuration command as greater than the `dot1x timeout quiet-period` interface configuration command setting, users were not authenticated into the guest VLAN when 802.1x authentication failed.
- CSCed87243

  If the VTP password is configured but the VTP domain name is not configured, and if the switch reloads twice, the switch now retains the VLAN information.
- 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 removed from the port.
- CSCee30022

  This message no longer appears when you add an aggregate policer to a policy map:

  ```
  BAD policymap info 9999999
  ```
- CSCee30090

  This message no longer appears when you modify a policer or remove an aggregate policer:

  ```
  Download failed for <class-name>
  Bad policymap info.
  ```
- CSCee30129

  When you add an aggregate policer to a policy-map class, the aggregate policer is no longer also added to another policy class within the same policy.
- CSCee37070

An 802.1x port in single-host mode with port security enabled will no longer go into the errdisable state and display the %DOT1X-5-SECURITY_VIOLATION message if another MAC is seen.

- CSCee37552

  The switch no longer fails when it executes the `shutdown` interface configuration command on an 802.1x enabled port.

- CSCee84918

  When DHCP snooping is enabled on the switch, clients attached to an interface move from one subnet to another, and a client attached to the switch sends a DHCP request to the previous subnet, the DHCP negative acknowledgement packet is no longer dropped by the switch.

- CSCef04854

  If you use the `no switchport` interface configuration command to configure a port as a routed port and then enable 802.1x on the port by using the `dot1x port-control auto` interface configuration command, 802.1x authentication no longer fails if you disable and then re-enable 802.1x on the port.

- CSCef09489

  The switch now correctly forwards Extensible Authentication Protocol (EAP) messages received from a RADIUS server to a client with no delay to the client.

- CSCef16610

  When IP source guard is configured and unconfigured on an interface several times, a memory leak no longer occurs.

- CSCef42734

  When a new 802.1x session is started, the switch now purges old state information, which prevents the switch from failing to authenticate due to stale State(24) field values.

- CSCef55486

  When the 802.1x accounting feature is configured, the switch no longer loses connectivity to the RADIUS server for an extended period of time, 802.1x transactions no longer time out, and switch reloads no longer occur.

- CSCef65587

  These error messages no longer appear randomly:

  ```
  %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
  ```

- CSCef78853

  Entering certain characters in some menu items in the device manager window could cause the front panel of a switch to not appear or error dialogs to appear. This situation occurred when a semicolon (;), single quotation mark (‘), or double quotation mark (“) was used as part of the hostname, port description, SNMP system location, SNMP system contact, SNMP community strings, Telnet password, or switch password.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCei76358

  Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

- CSCsb75533

  A switch running Cisco IOS release 12.2(25)SEB1 and a vendor type of “cevPortGigBaseLX” now displays the SNMP table “entAliasMappingTable”.

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 p-Class BladeSystem Release Notes* (part number 383623-001)
- *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Software Configuration Guide* (part number 380261-001)
- *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem System Message Guide* (part number 380260-001)
- *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem Hardware Installation Guide* (part number 380264-001)
- *Cisco Gigabit Ethernet Switch Module for HP p-Class BladeSystem 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

Obtaining technical support

For the name of the nearest HP authorized reseller:

- In the United States, see http://www.hp.com/service_locator.
- In other locations, see http://www.hp.com.

For HP technical support:

- In North America:
  - 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, see http://www.hp.com/support.
- Outside the United States and Canada, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, see http://www.hp.com/support.

Legal notices

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.