Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Release Notes, Cisco IOS Release 12.2(35)SE 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(35)SE

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

The system requirements are described in these sections:

Device Manager System Requirements

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

Hardware Requirements

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

Table 1 Minimum Hardware Requirements

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

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

Software Requirements

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

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

Table 2 Supported Operating Systems and Browsers

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

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

Cluster Compatibility

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

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

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

Upgrading the Switch Software

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

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

Finding the Software Version and Feature Set

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

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

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

Deciding Which Files to Use

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

Here are the filenames for this software release:

- cgesm-lanbase-tar.122-35.SE5.tar
- cgesm-lanbasek9-tar.122-35.SE5.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.

New Software Feature

This release supports Web authentication to authenticate a supplicant (client) that does not support IEEE 802.1x functionality. For more information, see the "Documentation Updates" section on page 22.

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 supports web authentication for authenticating a supplicant (client) that does not support IEEE 802.1x functionality. For more information, see the "Documentation Updates" section on page 22.

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
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 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

Configuration

These are the configuration limitations:

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

  This problem occurs under these conditions:

  - When the switch is booted 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)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

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

Ethernet

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

HSRP

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

IP

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

IP Telephony

These are the IP telephony limitations:

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

Multicasting

These are the multicasting limitations:

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

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

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

  There is no workaround. (CSCee16865)

QoS

These are the quality of service (QoS) limitations:

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

SPAN and RSPAN

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

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

  This is a hardware limitation: (CSCdy72835)

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

  This is a hardware limitation: (CSCdy81521)

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

  This is a hardware limitation: (CSCed24036)

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

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the LED to blink amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909)
- For trunk ports or access ports configured with 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100)

VLAN

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

Device Manager Limitations and Restrictions

These are the device manager limitations and restrictions:

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

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

Hardware Limitations and Restrictions

These are the hardware limitations and restrictions:

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

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

Device Manager Notes

These notes apply to the device manager:

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

  From Microsoft Internet Explorer:

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

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

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

	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. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

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

VLAN Interfaces and MAC Addresses

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

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

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

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

Documentation Notes

This section describes documentation notes related to this IOS release.

References to IOS Release Number

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

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

Open Caveats

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

- "Open IOS Caveats" section on page 13
- "Open Device Manager Caveats" section on page 17

Open IOS Caveats

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

- CSCee08109

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

  There is no workaround.

- CSCeg04311

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

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

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

These system messages also appear:

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

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

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

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

- CSCeg67844

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

  There is no workaround.

- CSCsb85001

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

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

- CSCsc26726

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

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

- CSCsd78044

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

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

- CSCsd85770

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

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

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

- CSCsd86177

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

  The workaround is to reload the switch.

- CSCse03859

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

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

- CSCse06827

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

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

- CSCse14774

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

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

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

- CSCsg18176

  When dynamic ARP inspection is enabled and IP validation is disabled, the switch drops ARP requests that have a source address of 0.0.0.0.

  The workaround is to configure an ARP access control list (ACL) that permits IP packets with a source IP address of 0.0.0.0 (and any MAC) address) and apply the ARP ACL to the desired DAI VLANs.

- CSCsg21537

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

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

- CSCsg30295

  When you configure an IP address on a switch virtual interface (SVI) with DCHP and enable DHCP snooping on the SVI VLAN, the switch SVI cannot obtain an IP address.

  The workaround is to not enable DCHP snooping on the SVI VLAN or to use a static IP address for the SVI.

- CSCsg79506

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

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

- CSCsg81334

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

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

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

This sections describes the caveats that have been resolved in these releases:

- "Resolved Caveats in Cisco IOS Release 12.2(35)SE5" section on page 17
- "Resolved Caveats in Cisco IOS Release 12.2(35)SE" section on page 18

Resolved Caveats in Cisco IOS Release 12.2(35)SE5

The are the resolved caveats in Cisco IOS Release 12.2(35)SE5:

- CSCed87897

  The output of the **show ip route** privileged EXEC command now correctly displays the default gateway.

- 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.

- CSCsi74508

  A switch no longer displays this error message when reading from or writing to the configuration file:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: write of 11 bytes to 10 bytes
  -Traceback= 0x41186A90 0x411A3960 0x411C1F88 0x413C24B8 0x4031EEDC 0x4032D144
  0x411C3974 0x41193D9C 0x4119420C 0x411DF55C 0x411C70AC 0x411E3184 0x425590F4
  0x4254BD7C 0x421B5CE0 0x421B5CC4
  ```

- CSCsi94450

  When DHCP snooping is enabled on a VLAN, the broadcast DHCP request is now correctly sent over the trusted port and the connected hosts correctly receive their IP addresses.

Resolved Caveats in Cisco IOS Release 12.2(35)SE

The are the resolved caveats in Cisco IOS Release 12.2(35)SE:

- CSCee22376

  When an SNMP version 3 user is configured with the encrypted option and password, the switch no longer reloads when the MIB object usmUserAuthKeyChange is set.

- CSCef94061

  If you entered the letter *i* by itself in the port description, the VLAN status column no longer displays only *i* ; this only occurred when you were using Device Manager through Netscape 7.1.

- CSCeg04311

  no longer 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 appeared:

  ```
  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
  ```

- CSCeg67844

  When using SNMP, the switch no longer returns an incorrect value of 65534 for the ciscoFlashPartitionFileCount MIB.

- CSCei63394

  When an IEEE 802.1x restricted VLAN is configured on a port and a hub with multiple devices are connected to that port, syslog messages are now generated.

  This is not a supported configuration. Only one host should be connected to an IEEE 802.1x restricted VLAN port.

- CSCsb12598

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsb40304

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- CSCsb56438

  An extra index no longer appears in the port table of the ciscoStpExtensions MIB.

- CSCsb75245

  When you configure a Cisco IP Phone to use Network Admission Control, the CDP packet is no longer delayed, and the phone is no longer identified as an agentless host without an identity profile.

- CSCsb74648

  When a Cisco device is configured for Network Admission Control and the EAP over UDP port number changes from its default value and then changes back with the *eou* default switch configuration command, the port change now takes effect.

- CSCsc05371

  When you configure a MAC address filter by entering the **mac-address-table static vlan drop** global configuration command, IEEE 802.1X no longer authenticates supplicants using that address. If a supplicant with that address is authenticated, its authorization is revoked.

- CSCsc26726

  The interfaces GigabitEthernet0/23 and 0/24 now link to another switch or host when the interface speed is set to an explicit value or auto-MDIX is disabled.

- CSCsc29225

  When you remove the bridge topology change trap with the **no snmp-server enable traps bridge topologychange** configuration command, the stpx root-inconsistency trap is now active.

- CSCsd78044

  When IGMP snooping is enabled and an EtherChannel member interface goes down, the switch now forwards multicast traffic on the rest of the EhternetChannel member interfaces.

- CSCsc83583

  When you enter the **show interfaces transceiver properties** privileged EXEC command for a Gigabit Ethernet dual-media interface and the interface is set to **media-type rj45**, the output now shows the correct attached SFP module. This only applies to GigabitEthernet0/17 to 0/20.

- CSCsd85587

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

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

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

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

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

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

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

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

- CSCsd85770

  When you apply the **mls qos trust dscp** global configuration command to a port, this error message no longer appears:

  ```
  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
  ```

- CSCsd86177

  When you remove and reconfigure a loopback interface, it no longer appears in the ifTable.

- CSCsd92405

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

- 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 no longer fail 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.

- 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

Documentation Updates

This section provides these updates:

Updates to Software Configuration Guide

This section was added to the "Configuring EtherChannels" chapter:

When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. In previous releases, the incompatible ports were suspended. Beginning with Cisco IOS Release 12.2(35)SE, instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

Update to the "Configuring IEEE 802.1x chapter

These sections were added to the "Configuring IEEE 802.1x" chapter:

Using Web Authentication

You can use a web browser to authenticate a client that does not support IEEE 802.1x functionality.

You can configure a port to use only web authentication. You can also configure the port to first try and use IEEE 802.1x authentication and then to use web authorization if the client does not support IEEE 802.1x authentication.

Web authentication requires two Cisco Attribute-Value (AV) pair attributes:

- The first attribute, `priv-lvl=15`, must always be set to *15*. This sets the privilege level of the user who is logging into the switch.
- The second attribute is an access list to be applied for web authenticated hosts. The syntax is similar to IEEE 802.1X per-user ACLs. However, instead of `ip:inacl`, this attribute must begin with `proxyacl`, and the `source` field in each entry must be `any`. (After authentication, the client IP address replaces the `any` field when the ACL is applied.)

  For example:

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

Note The *proxyacl* entry determines the type of allowed network access.

For more information, see the "Configuring Web Authentication" section on page 23.

Configuring Web Authentication

Beginning in privileged EXEC mode, follow these steps to configure authentication, authorization, accounting (AAA) and RADIUS on a switch before configuring web authentication. The steps enable AAA by using RADIUS authentication and enable device tracking.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.

	Command	Purpose

Step 3	aaa authentication login default group radius	Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see Chapter 9, "Configuring Switch-Based Authentication."
		The console prompts you for a username and password on future attempts to access the switch console after entering the **aaa authentication login** command. If you do not want to be prompted for a username and password, configure a second login authentication list:
		`Switch# config t`
		`Switch(config)# aaa authentication login line-console none`
		`Switch(config)# line console 0`
		`Switch(config-line)# login authentication line-console`
		`Switch(config-line)# end`

Step 4	**aaa authorization auth-proxy default group radius**	Use RADIUS for authentication-proxy (auth-proxy) authorization.
Step 5	**radius-server host key** *radius-key*	Specify the authentication and encryption key for RADIUS communication between the switch and the RADIUS daemon.
Step 6	**radius-server attribute 8 include-in-access-req**	Configure the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets.
Step 7	**radius-server vsa send authentication**	Configure the network access server to recognize and use vendor-specific attributes (VSAs).
Step 8	**ip device tracking**	Enable the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.
Step 9	end	Return to privileged EXEC mode.

This example shows how to enable AAA, use RADIUS authentication and enable device tracking:

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
Switch(config)# radius-server host key key1
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# radius-server vsa send authentication
Switch(config)# ip device tracking
Switch(config) end
```

Beginning in privileged EXEC mode, follow these steps to configure a port to use web authentication:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip admission name** *rule* **proxy http**	Define a web authentication rule. **Note** The same rule cannot be used for both web authentication and NAC Layer 2 IP validation.

	Command	Purpose
Step 3	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 4	**switchport mode access**	Set the port to access mode.
Step 5	**ip access-group** *access-list* **in**	Specify the default access control list to be applied to network traffic before web authentication.
Step 6	**ip admission** *rule*	Apply an IP admission rule to the interface.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config interface** *interface-id*	Verify your configuration.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure only web authentication on a switch port:

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# ip access-group policy1 in
Switch(config-if)# ip admission rule1
Switch(config-if)# end
```

Beginning in privileged EXEC mode, follow these steps to configure a switch port for IEEE 802.1x authentication with web authentication as a fallback method:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip admission name** *rule* **proxy http**	Define a web authentication rule.
Step 3	**fallback profile** *fallback-profile*	Define a fallback profile to allow an IEEE 802.1x port to authenticate a client by using web authentication.
Step 4	**ip access-group** *policy* **in**	Specify the default access control list to apply to network traffic before web authentication.
Step 5	**ip admission** *rule*	Associate an IP admission rule with the profile, and specify that a client connecting by web authentication uses this rule.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 8	**switchport mode access**	Set the port to access mode.
Step 9	**dot1x port-control auto**	Enable IEEE 802.1x authentication on the interface.
Step 10	**dot1x fallback** *fallback-profile*	Configure the port to authenticate a client by using web authentication when no IEEE 802.1x supplicant is detected on the port. Any change to the fallback-profile global configuration takes effect the next time IEEE 802.1x fallback is invoked on the interface. **Note** Web authorization cannot be used as a fallback method for IEEE 802.1x if the port is configured for multidomain authentication.

	Command	Purpose
Step 11	**exit**	Return to privileged EXEC mode.
Step 12	**show dot1x interface** *interface-id*	Verify your configuration.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback method.

```
Switch(config) configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback fallback1
Switch(config-if)# end
```

For more information about the **ip admission name** and **dot1x fallback** commands, see the command reference for this release.

Updates to the Command Reference

These commands were added:

- dot1x fallback, page 27
- fallback profile, page 28
- ip admission, page 29
- ip admission name proxy http, page 30
- show fallback profile, page 31

dot1x fallback

Use the **dot1xfallback** interface configuration command on the switch stack or on a standalone switch to configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. To return to the default setting, use the **no** form of this command.

dot1x fallback *profile*

no dot1x fallback

Syntax Description

profile	Specify a fallback profile for clients that do not support IEEE 802.1x authentication.

Defaults

No fallback is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

You must enter the **dot1x port-control** auto interface configuration command on a switch port before entering this command.

Examples

This example shows how to specify a fallback profile to a switch port that has been configured for IEEE 802.1x authentication:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
show dot1x [interface *interface-id***]**	Displays IEEE 802.1x status for the specified port.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a port
ip admission name proxy http	Enable web authentication globally on a switch

fallback profile

Use the **fallback profile** global configuration command on the switch stack or on a standalone switch to create a fallback profile for web authentication. To return to the default setting, use the **no** form of this command.

fallback profile *profile*

no fallback profile

Syntax Description

profile	Specify the fallback profile for clients that do not support IEEE 802.1x authentication.

Defaults

No fallback profile is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The fallback profile is used to define the IEEE 802.1x fallback behavior for IEEE 802.1x ports that do not have supplicants. The only supported behavior is to fall back to web authentication.

After entering the **fallback profile** command, you enter profile configuration mode, and these configuration commands are available:

- **ip:** Create an IP configuration.
- **access-group:** Specify access control for packets sent by hosts that have not yet been authenticated.
- **admission:** Apply an IP admission rule.

Examples

This example shows how to create a fallback profile to be used with web authentication:

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

You can verify your settings by entering the **show running-configuration** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch
shot dot1x [interface *interface-id*]	Displays IEEE 802.1x status for the specified port.
show fallback profile	Display the configured profiles on a switch.

ip admission

Use the **ip admission** interface configuration command to enable web authentication. You can also use this command in fallback-profile mode. Use the **no** form of this command to disable web authentication.

ip admission *rule*

no ip admission

Syntax Description

rule	Apply an IP admission rule to the interface.

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

Examples

This example shows how to apply a web authentication rule to a switchport:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Enable web authentication on a port
ip admission name proxy http	Enable web authentication globally on a switch
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the *Network Admission Control Software Configuration Guide* on Cisco.com.

ip admission name proxy http

Use the **ip admission name proxy http** global configuration command to enable web authentication. Use the **no** form of this command to disable web authentication.

ip admission name *proxy http*

no ip admission name *proxy htt***p**

Syntax Description

This command has no arguments or keywords.

Defaults

Web authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The **ip admission name proxy http** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission** *web-rule* interface configuration commands to enable web authentication on a specific interface.

Examples

This example shows how to configure only web authentication on a switchport:

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switchport.

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a port
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the *Network Admission Control Software Configuration Guide* on Cisco.com.

show fallback profile

Use the **show fallback profile** privileged EXEC command to display the fallback profiles that are configured on a switch.

show fallback profile [append | begin | exclude | include | { [redirect | tee] ***url*** } *expression]*

Syntax Description

| append	(Optional) Append redirected output to a specified URL
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
| redirect	(Optional) Copy output to a specified URL.
| tee	(Optional) Copy output to a specifed URL.
expression	Expression in the output to use as a reference point.
url	Specified URL where output is directed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

Use the **show fallback** profile privileged EXEC command to display profiles that are configured on the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show fallback profile** command:

```
switch# show fall profile
Profile Name: dot1x-www
-----------------------------------
Description       : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
-----------------------------------
Description       : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
-----------------------------------
Description       : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch
show dot1x [interface *interface-id*]	Displays IEEE 802.1x status for the specified port.

Updates to the System Message Guide

These system messages were added to the system message guide:

Error Message `DOT1X-5-SECURITY_VIOLATION: Security violation on the interface [chars], new MAC address [enet] is seen.`

Explanation A host on the specified interface is trying to access the network or to authenticate in a host mode that does not support the number of hosts attached to the interface. This is a security violation, and the port is put in the error-disabled state.

Recommended Action Ensure that the interface is configured to support the number of attached hosts. Enter the **shutdown** interface configuration command and then the **no shutdown** interface configuration command to restart the port.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN.`

Explanation The IEEE 802.1x-assigned VLAN on a port cannot be the same as the voice VLAN. [dec] is the data VLAN ID, and [chars] is the port.

Recommended Action Configure either a different voice VLAN or a different IEEE 802.1x-assigned access VLAN on the interface. The authentication then proceeds normally on the next retry.

Error Message `FRNTEND_CTRLR-1-MGR_TXQ_FULL: The front end controller Tx queue reached watermark level`

Explanation There are too many messages in the queue between the front-end controller and the switch software.

Recommended Action Try reloading the switch. If this does not resolve the issue, this might be a hardware problem. Contact the Cisco technical support representative.

Error Message `GBIC_SECURITY_CRYPT-4-ID_MISMATCH: Identification check failed for GBIC in port [chars]`

Explanation The small form-factor pluggable (SFP) module was identified as a Cisco SFP module, but the system could not verify its identity. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software. Otherwise, verify that the SFP module was obtained from Cisco or from a supported vendor.

Error Message `GBIC_SECURITY_CRYPT-4-UNRECOGNIZED_VENDOR: GBIC in port [chars] manufactured by an unrecognized vendor`

Explanation The small form-factor pluggable (SFP) module was identified as a Cisco SFP module, but the switch could not match its manufacturer with one on the known list of Cisco SFP module vendors. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software.

Error Message `GBIC_SECURITY_CRYPT-4-VN_DATA_CRC_ERROR: GBIC in port [chars] has bad crc`

Explanation The small form-factor pluggable (SFP) module was identified as a Cisco SFP module, but it does not have a valid cyclic redundancy check (CRC) in the EEPROM data. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software. Even if the switch does not recognize the SFP module, it might still operate properly but have limited functionality.

Error Message `PHY-4-UNSUPPORTED_SFP_CARRIER: Unsupported SFP carrier module found in [chars]`

Explanation The switch has identified the small form-factor pluggable (SFP) module as an unsupported non-Cisco SFP module. [chars] is the interface.

Recommended Action Remove the unsupported SFP module, and use a supported module.

Error Message `PORT_SECURITY-6-ADDR_REMOVED: Address [dec]:[enet] exists on port [chars]. It has been removed from port [chars].`

Explanation A routed port is reconfigured as a switch port. The address in the previous switch configuration conflicts with the running configuration and has been deleted. [dec]:[enet] is the MAC address of the port. [chars] is the reconfigured port.

Recommended Action No action is required.

Error Message `WCCP-5-SERVICEFOUND: Service [chars] acquired on WCCP Client [IP_address]`

Explanation Web Cache Communication Protocol (WCCP) has found a service on the specified WCCP client. [chars] is the name of the service, and [IP_address] is the client IP address.

Recommended Action No action is required.

Error Message `WCCP-1-SERVICELOST: Service [chars] lost on WCCP Client [IP_address]`

Explanation WCCP has lost the service associated with the specified WCCP client. [chars] is the name of the service, and [IP_address] is the client IP address.

Recommended Action Verify the operational state of the WCCP client.

These system messages were updated in the system message guide:

Error Message `EC-5-CANNOT_BUNDLE_LACP: [chars] is not compatible with aggregators in channel [dec] and cannot attach to them ([chars]).`

Explanation The port has different port attributes than the port channel or ports within the port channel. [chars] is the incompatible port. [chars] is the short interface name, such as Gi1/0/1 on a Catalyst 3750 switch, [dec] is the channel group number, and the last [chars] is the reason.

Recommended Action For the port to join the bundle, change the port attributes so that they match the port.

Error Message `EC-5-DONTBNDL: [chars] suspended: incompatible remote port with [chars]`

Recommended Action The configuration of the remote port differs from the configuration of other remote ports in the bundle. A port can only join the bundle when its global configuration and the configuration of the remote port are the same as other ports in the bundle. The first [chars] is the suspended local interface, and the second [chars] is the local interface that is already bundled.

Error Message `PORT_SECURITY-6-VLAN_REMOVED: VLAN [int] is no longer allowed on port [chars]. Its port security configuration has been removed.`

Explanation A configured VLAN has been excluded either due to a port-mode change or an allowed VLAN list change and is removed from the configuration. [int] is the VLAN ID, and [chars] is the switch port assigned to the VLAN.

Recommended Action No action is required.

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).
- 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).