Cisco Gigabit Ethernet Switch Module for HP BladeSystem p-Class Release Notes, Cisco IOS Release 12.2(44)SE and Later

Revised March 25, 2009

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

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.122-44.SE6.tar
- cgesm-lanbasek9-tar.122-44.SE6.tar

Upgrading a Switch by Using the Device Manager

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

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

Upgrading a Switch by Using the CLI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recovering from a Software Failure

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

Installation Notes

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

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

New Software Features

The *, *ip-address,* **interface** *interface-id,* and **vlan** *vlan-id* keywords were introduced to the **clear ip dhcp snooping** command in this release.

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
Configuration replacement and rollback	12.2(40)SE
IP Service Level Agreements (IP SLAs) responder	12.2(40)SE
Private VLANs	12.2(40)SE
Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE
Support for the CISCO-MAC-NOTIFICATION-MIB	12.2(40)SE
VLAN Flex Links load balancing	12.2(37)SE
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE
VLAN aware port security	12.2(37)SE
Support for DHCP snooping statistics	12.2(37)SE
Support for auto rendezvous point (auto-RP) for multicast	12.2(37)SE
Web authentication	12.2(35)SE
Support for DSCP transparency	12.2(25)SE1
Support for VLAN-based QoS and hierarchical policy maps on SVIs	12.2(25)SE1
Device manager	12.2(25)SE1
Support for SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE1
802.1x accounting and MIBs (IEEE8021-PAE-MIB and CISCO-PAE-MIB)	12.2(25)SE1
Flex Links	12.2(25)SE1
HTTP software upgrade (device manager only)	12.2(25)SE1
SFP module diagnostic-management interface	12.2(25)SE1
Smartports macros	12.2(25)SE1

Limitations and Restrictions

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

This section contains these limitations:

Cisco IOS Limitations

These limitations apply to CGESM switch:

Configuration

These are the configuration limitations:

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

  This problem occurs under these conditions:

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

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

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

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

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

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

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

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)
- When system jumbo MTU size is configured on a switch and the egress ports can support jumbo frames, the egress SPAN jumbo frames are not forwarded to the SPAN destination ports.

  There is no workaround. (CSCsj21718)

Ethernet

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

HSRP

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

IP

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

IP Telephony

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

- 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

- 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

- 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

- 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)
- When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state. (CSCse06827)

Device Manager Limitations and Restrictions

- 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

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

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

Important Notes

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

- "Cisco IOS Notes" section on page 11
- "Device Manager Notes" section on page 12

Cisco IOS Notes

These notes apply to Cisco IOS software:

- Cisco IOS Release 12.2(40)SE and later

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

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

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

Device Manager Notes

These notes apply to the device manager:

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

  From Microsoft Internet Explorer:

  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the "Temporary Internet files" area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.

- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

  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

References to Cisco IOS Release 12.2(25)SE

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

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

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

Open Caveats

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

- "Open IOS Caveats" section on page 14
- "Open Device Manager Caveats" section on page 15

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.

- 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.

- CSCsi70454

  The configuration file used for the configuration replacement feature requires the character string *end\n* at the end of the file. The Windows Notepad text editor does not add the *end\n* string, and the configuration rollback does not work.

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

  - Do not use a configuration file that is stored by or edited with Windows Notepad.
  - Manually add the character string *end\n* to the end of the file.

- CSCsj74022

  The switch does not correctly update the entPhysicalChildIndex objects from the ENTITY-MIB, and some of the entPhysicalChildIndex entries are missing from the table. This adversely affects network management applications such as CiscoWorks CiscoView because they cannot manage the switch.

  There is no workaround.

Open HP Caveats

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

- rQm 263546

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

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

- rQm 266129

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

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

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 section describes the caveats that have been resolved in these releases:

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE6

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the "workarounds" section of the advisory. The advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

- CSCso75640

  When MAC authentication bypass (MAB) authentication fails, a memory leak no longer occurs.

- CSCsq89564

  When a VLAN is assigned for IEEE 802.1x authentication and no VLAN is assigned for other types of authentication (such as user authentication or reauthentication), the 802.1x VLAN assignment no longer persists across subsequent authentication attempts.

- CSCsr54797

  When the switch uses HTTP (web-based) authentication, a memory leak no longer occurs after authorization and policy download.

- CSCsx42798

  A switch no longer displays processor memory-allocation failure messages under these conditions:

  - The switch is running IOS release 12.2(44)SE4 or 12.2(44)SE5.
  - Authentication, authorization, and accounting (AAA) is configured on the switch.
  - Memory in the primary processor pool is depleted.

Note If the hardware configuration is not a switch stack, AAA requests might fail and the switch might experience high CPU usage for the authentication manager process. In addition, if the hardware configuration is a switch stack and 802.1x, web authentication, or MAC address bypass (MAB) are configured, the switch software might reload after reporting the memory-allocation failure.

This is resolved in Cisco IOS 12.2(44)SE6 and later.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE5

- CSCsd73245

  Excessive IPRT-3-PATHIDX error messages no longer appear in the log file.

- CSCsf10850

  When configuring an IP SSH version 2 connection, you can no longer create an RSA key that is less than 768 bits.

- CSCso63475

  A switch now boots correctly after a software reload or power cycle. In previous releases, under some rare circumstances, the image would be truncated to zero bytes and the switch would not boot.

- CSCsu10229

  The cdpCacheAddress value now appears in a GLOBAL_UNICAST address.

- CSCsu40077

  The switch now correctly processes ingress traffic when a port is configured with a short 802.1x **tx-period timer** value (such as **dot1x timeout tx-period 3**).

- CSCsu47056

  The username is now properly logged when the **remote command** privileged EXEC command is used to configure a cluster member.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE3

- CSCee55603

  An SNMP access-control list (ACL) now works correctly on virtual routing and forwarding (VRF) interfaces.

- CSCso75052

  An end host no longer remains in the guest VLAN after an IEEE 802.1x authentication.

- CSCsq71492

  The switch no longer reloads with an address error if the TACACS+ server sends an authentication error when the access control system is configured and a timeout request occurs.

- CSCsr55949

  When IEEE 802.1x port-based authentication is enabled on the switch, Extensible Authentication Protocol (EAP) notification packets from the supplicant are no longer discarded.

- CSCsu04337

  In environments using Layer 2 IP Network Admission Control (NAC), long downloadable ACLs (dACLs) with source or destination Layer 4 ports no longer cause unpredictable events in which all traffic is dropped and URL redirects are not enforced.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE2

- CSCsg91027

  When the logging event-spanning-tree interface configuration command is configured and logging to the console is enabled, a topology change no longer generates a large number of logging messages.

- CSCsl76599

  The switch no longer unexpectedly reloads while configured with IEEE 802.1x authentication and the MAC authentication bypass feature.

- CSCsl77063

  When you enable detection of Cisco IP phones by entering the **switchport voice detect cisco-phone** interface configuration command, the interface is no longer disabled if you connect a third-party IP phone is connected to the interface.

Note This command was designed to work with Cisco IP phones; you should not enable it on interfaces connected to third-party IP phones.

- CSCsl93313

  When you configure a port channel as trusted by entering the **ip dhcp snooping trust** interface configuration command, the configuration is no longer lost when the link goes from down to up.

- CSCsm08603

  This traceback error no longer appears when you enter the **show aaa subscriber profile** privileged EXEC command:

```
*Mar 2 01:50:41.127: %PARSER-3-BADSUBCMD: Unrecognized subcommand 10 in exec command
'show aaa subscriber profile WORD'
-Traceback= D003B4 D00AC8 C908A0 C2F040 C8CA18 CB8984 93B670 932338
```

Note In Cisco IOS Release 12.2(44)SE2 and later, the **subscriber** keyword is no longer supported. (The **show aaa subscriber profile** command is not supported, and you cannot configure the aaa subscriber profile command.)

- CSCsm26406

  Enhanced IGRP (EIGRP) now works correctly when you enter the **ip authentication key-chain eigrp** interface configuration command.

- CSCsm61718

  A switch no longer unexpectedly reloads when you configure two or more authentication, authorization, and accounting (AAA) broadcast groups.

- CSCso75848

  The switch no longer experiences a memory leak during an HTTP core process.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE1

- CSCec51750

  A router that is configured for HTTP and voice-based services no longer unexpectedly reloads due to memory corruption.

- CSCek57932

  Cisco uBR10012 series devices automatically enable Simple Network Management Protocol (SNMP) read/write access to the device if configured for linecard redundancy. This can be exploited by an attacker to gain complete control of the device. Only Cisco uBR10012 series devices that are configured for linecard redundancy are affected.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml.

- CSCsd45672

  When AAA is enabled and you use the **aaa group server radius** *group-name* global configuration command to put the switch in server group configuration mode, entering the **server-private** command no longer causes the switch to reload.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

- CSCse56800

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsg22426

  A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml.

- CSCsg91306

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsh12480

  Cisco IOS software configured for Cisco IOS firewall Application Inspection Control (AIC) with a HTTP configured application-specific policy are vulnerable to a Denial of Service when processing a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

  Cisco has released free software updates that address this vulnerability.

  A mitigation for this vulnerability is available. See the "Workarounds" section of the advisory for details.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml.

- CSCsh46990

  The switch no longer reloads when you use the **aaa authentication eou default group radius enable** global configuration command to configure an EAP over UDP (EOU) method list.

- CSCsh48879

  A vulnerability exists in the Cisco IOS software implementation of Layer 2 Tunneling Protocol (L2TP), which affects limited Cisco IOS software releases.

  Several features enable the L2TP mgmt daemon process within Cisco IOS software, including but not limited to Layer 2 virtual private networks (L2VPN), Layer 2 Tunnel Protocol Version 3 (L2TPv3), Stack Group Bidding Protocol (SGBP) and Cisco Virtual Private Dial-Up Networks (VPDN). Once this process is enabled the device is vulnerable.

  This vulnerability will result in a reload of the device when processing a specially crafted L2TP packet.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the "workarounds" section of the advisory.

  The advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml.

- CSCsi17020

  A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml.

- CSCsj85065

  A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability.

  Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml.

- CSCsk42759

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsl34355

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

- CSCsl62609

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsm41883

  High CPU usage (greater than 90 percent) no longer occurs on the switch when you first connect a new device.

- CSCsm57520

  A switch no longer unexpectedly reloads when you configure the switch ports as dynamic ports by using the VLAN Membership Policy Server (VMPS).

- CSCsq13348

  The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

  Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

  NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosips.shtml.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(44)SE

These caveats were resolved in Cisco IOS Release 12.2(44)SE:

- CSCeg67844

  The switch no longer returns an incorrect value for the ciscoFlashPartitionFileCount MIB.

- CSCsb85001

  When traffic passes through a VMPS port and you enter the **shut** interface configuration command, a dynamic VLAN is now assigned.

- CSCsc26726

  Gigabit interfaces 0/23 and 0/24 now link up with another switch when the interface speed is set to an explicit value. In previous releases, these ports would only link up with another switch if the ports on that switch were set to autonegotiate.

- CSCsc30733

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

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

- CSCsd01180

  The switch no longer reloads when you use a Kron command scheduler routine to automatically copy configuration data using the Secure Copy Protocol (SCP). (Kron is a Cisco IOS utility for scheduling non-prompting CLI commands to execute at a later time.)

- CSCsd78044

  When IGMP snooping is enabled and an EtherChannel member interface fails, the switch no longer stops forwarding multicast traffic on the EtherChannel. In previous releases, this occurred when multicast routing was enabled and the EtherChannel interface was a member of a multicast group not directly connected (that is, the multicast group that did not have the C flag set in the **show ip mroute** privileged EXEC command output).

- CSCsd85770

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

  ```
  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
  ```

- CSCse14774

  When 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.

- CSCsg21537

  When MAC addresses are learned on an EtherChannel port, the addresses are now correctly deleted from the MAC address table.

- 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 can now obtain an IP address.

- CSCsg70630

  A switch with the Dynamic ARP Inspection feature enabled no longer experiences the issue that triggered the display of *buffer sharecount* messages under certain patterns of ARP packet traffic.

- CSCsh74395

  When a VLAN includes multiple MAC addresses, the number of MAC addresses shown in SNMP now matches the output of the **show mac-address count vlan** *vlan-id* privileged EXEC command.

- CSCsi08513

  MAC flap-notification no longer occurs when a switch is running VLAN bridge spanning-tree protocol (STP) and fallback bridging is configured on the VLANs running STP.

- CSCsi10584

  Multiple Spanning-Tree Protocol (MSTP) convergence time has been improved for Cisco IOS Release 12.2.

- CSCsi63999

  Changing the spanning tree mode from MSTP to other spanning modes no longer causes tracebacks.

- CSCsi77705

  Broadcast storm control now works correctly on IEEE 802.1Q trunk ports.

- CSCsi78737

  The cpmCPURising Threshold traps on the switch are no longer missing the cpmProcExtUtil5SecRev and cpmProcessTimeCreated trap components. Note that although the components were missing from the traps, the PROCESS MIB was still populating the objects.

- CSCsj22994

  ACLs are now configured correctly when they contain ICMP codes 251 to 255.

- CSCsj47067

  If you upgrade from Cisco IOS Release 12.2(35)SE1 to Release 12.2(37)SE, a security violation no longer occurs when:

  - You enter the **switchport port-security maximum 1 vlan access** interface configuration command.
  - An IP phone with a PC behind it is connected to an access port with port security.

- CSCsj52956

  The TxBufferFullDropCount counter no longer increments when the switch is a standalone switch.

- CSCsj53001

  The Total- output-drops field in the **show interfaces** privileged EXEC command output now displays accurate ASIC drops.

- CSCsj64882

  When IGMP snooping is enabled, CGMP interoperability mode now works as it should when the upstream multicast router is set up correctly with PIM and IP CGMP.

- CSCsj77933

  If you enter a space before a comma in the **define interface-range** or the **interface range** global configuration command, the space before the comma is now saved in the switch configuration.

- CSCsj87991

  A switch configured for Link Layer Discovery Protocol (LLDP) now correctly reports the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes.

- CSCsj90406

  When VTP pruning is enabled, the switch no longer might experience high CPU usage (greater than 90 percent) for up to 20 minutes after the link comes up simultaneously on multiple trunk ports.

- CSCsk25175

  When the switch has VTP pruning and an RSPAN session configured, the RSPAN VLAN traffic is now correctly pruned as set up by the VTP pruning configuration.

- CSCsk38083

  When UDLD is enabled on a Layer 2 interface, and the native VLAN for the port is not configured as a VLAN on the switch, UDLD no longer puts the port into an error-disabled state.

- CSCsk67520

  If you enter the **hostname** global configuration command followed by a hostname that contains illegal characters, for example, one that appears to be an IP address, the switch now displays a warning message, but the specified hostname is configured.

- CSCsi85257

  A Cisco IP Phone now works correctly when it is connected to a port that is configured with CDP bypass and multidomain authentication (MDA).

- CSCsk62010

  A switch no longer fails when you enter the **show interfaces vlan** *vlan-id* **switchport** privileged EXEC command.

- CSCsl33304

  Web authentication no longer stops working when IEEE 802.1X re-authentication is enabled and the re-authentication timer expires.

Documentation Updates

This section provides updates to the product documentation:

Update to the Software Configuration Guide

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

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

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

System Messages Guide

These are the documentation updates for the system modesties guide:

New System Messages

These system messages have been added.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]`

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. [enet] is the supplicant MAC address, and [chars] is the interface. This message might appear if the IEEE 802.1x feature is enabled.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, manually remove it from that port.

Error Message `SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans`

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message `SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans`

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message `SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].`

Explanation The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

Error Message `VQPCLIENT-2-TOOMANY: Interface [chars] shutdown by active host limit.`

Explanation The system has shut down the specified interface because too many hosts have requested access to that interface. [chars] is the interface name.

Recommended Action To enable the interface, remove the excess hosts, and enter the **no shutdown** interface configuration command.

Error Message `VQPCLIENT-3-VLANNAME: Invalid VLAN [chars] in response.`

Explanation The VLAN membership policy server (VMPS) has specified a VLAN name that is unknown to the switch. [chars] is the VLAN name.

Recommended Action Ensure that the VLAN exists on the switch. Verify the VMPS configuration by entering the **show vmps** privileged EXEC command.

Error Message `WCCP-5-CACHEFOUND: Web Cache [IP_address] acquired.`

Explanation The switch has acquired the specified web cache. [IP_address] is the web cache IP address.

Recommended Action No action is required.

Error Message `WCCP-1-CACHELOST: Web Cache [IP_address] lost.`

Explanation The switch has lost contact with the specified web cache. [IP_address] is the web cache IP address.

Recommended Action Verify the operation of the web cache by entering the **show ip wccp web-cache** privileged EXEC command.

Changed System Messages

This system message has changed (both explanation and action).

Error Message `EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.`

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration.

Related Documentation

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

http://www.hp.com/support

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

Cisco IOS Release 12.2 documentation is available at

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

Technical support

Before you contact HP

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

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Applicable error messages

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

HP contact information

For the name of the nearest HP authorized reseller:

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

For HP technical support:

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