Release Notes for Cisco Catalyst Blade Switch 3120 for HP, Cisco IOS Release 12.2(55)SE and Later

Revised March 28, 2012

Cisco IOS Release 12.2(55)SE runs on the Cisco Catalyst Blade Switch 3120 for HP switches. These switches support stacking through Cisco StackWise Plus technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(53)SE and later and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 4.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://www.cisco.com/cisco/web/download/index.html

For the complete list of the Cisco Catalyst Blade Switch 3120 for HP documentation, see the "Related Documentation" section on page 38.

Note References in this document to the CBS3120G-S and CBS3120X-S switches also apply to the CBS3125G-S and CBS3125X-S switches, respectively.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

System Requirements

Hardware Supported

Table 1 Cisco Catalyst Blade Switch 3120 for HP Supported Hardware

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
CBS3120G-S and CBS3120X-S	• 18 internal Gigabit Ethernet 1000BASE-X downlink ports that connect to the blade enclosure. • 4 Gigabit Ethernet (RJ-45) uplink ports • 4 RJ-45 SFP module slots[1]/ 2 10-Gigabit Ethernet X2 module slots • 1 Ethernet management port (Fa0) used only for switch module management traffic	Cisco IOS Release 12.2(40)EX1
Cisco X2 transceiver modules	X2-10GB-SR X2-10GB-LRM X2-10GB-CX4 X2-10GB-LR X2-10GB-LX4	12.2(40)EX3 12.2(46)SE

Table 1 Cisco Catalyst Blade Switch 3120 for HP Supported Hardware (continued)

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
SFP modules[2]	GLC-T GLC-SX-MM GLC-LH-SM	12.2(40)EX3
Supports OneX (CVR-X2-SFP10G) and these SFP+ modules	SFP-10G-SR SFP-10G-LR SFP-10G-LRM Only version 02 or later CX1[3] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	Cisco IOS Release 12.2(53)SE

1. X2 module supported only on the CBS3120X-S model
2. SFP = small form-factor pluggable
3. The CX1 cables are used with the OneX converters.

Caution The Cisco Catalyst Blade Switch 3120 for HP switch modules do not support switch stacks with other types of blades switches as members. Combining the Cisco Catalyst Blade Switch 3120 for HP with other types of blade switches in a switch stack might cause the switch to work improperly or to fail.

Device Manager System Requirements

Hardware Requirements

Table 2 lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1-GB DRAM.

Software Requirements

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

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

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

Cisco Network Assistant Compatibility

Cisco IOS 12.2(40)EX1 and later is only compatible with Cisco Network Assistant 5.3 and later. You can download Network Assistant from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

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

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** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base feature set or IP services feature set) and does not change if you upgrade the software license.

You can also 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 combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined 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.

Note To use the IPv6 routing and IPv6 ACL features on the Cisco Catalyst Blade Switch 3120 for HP, you must purchase the IP services software license from Cisco.

Table 3 Cisco IOS Software Image Files

Filename	Description
cbs31x0-universal-tar.122-55.SE.tar	Cisco Catalyst Blade Switch 3120 for HP universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch.
cbs31x0-universalk9-tar.122-55.SE.tar	Cisco Catalyst Blade Switch 3120 for HP universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

The universal software images support multiple feature sets. Use the software activation feature to deploy a software license and to enable a specific feature set. For information about software activation, see the *Cisco Software Activation for HP* document on Cisco.com:

http://www.cisco.com/en/US/products/ps6748/products_installation_and_configuration_guides_list.html

Archiving Software Images

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

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time-consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. 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 combined 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.

To download software, follow these steps:

Step 1 Use Table 3 on page 5 to identify the file that you want to download.

Step 2 Download the software image file:

a. If you are a registered customer, go to this URL and log in.

http://www.cisco.com/cisco/web/download/index.html

b. Navigate to **Switches > Blade Switches.**

c. Navigate to your switch model.

d. Click **IOS Software**, then select the latest IOS release.

Download the image you identified in Step 1.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

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

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

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

Step 6 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:

```
Switch# 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/cbs31x0-universal-tar.122-40.EX1.tar
```

You can also 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 additional recovery procedures, see the "Troubleshooting" chapter in the 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 switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Software Features

- Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices, such as the Cisco Telepresence System and Cisco Surveillance Camera.
- Support for CDP and LLDP enhancements for exchanging location information with video end points for dynamic location-based content distribution from servers.
- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs configured.
- Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.
- Support for the Security Group Tag (SCT) Exchange Protocol (SXP) component of Cisco TrustSec, a security architecture using authentication, encryption, and access control.
- AAA guarantee-first support for enabling or disabling system accounting as the first record.
- An option to suppress verbose 802.1x, authentication manager, and MAC authentication bypass syslog messages.
- Support for Embedded Event Manager (EEM) in the IP base image.
- Support for QoS class-default policy placement.

- The IP Base image supports OSPF for routed access to enable customers to extend Layer 3 routing capabilities to the access or wiring closet. The IP services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions.
- MAC move to allow hosts (including the hosts connected to an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port as a completely new MAC address.

  MAC replace can be configured so that when a host disconnects from a port without ending its session, the session can be ended and the authentication sequence reset when a new MAC address connects to the port.
- Support for increasing the NVRAM buffer size for saving large configuration files.
- ARP tracking probe enhancement to specify a source IP address for a VLAN.
- Network Edge Access Topology (NEAT) controls the supplicant port during the supplicant authentication period. When you connect a supplicant switch to the authenticator switch, the authenticator port could be error-disabled when receiving Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets and the supplicant switch is not authenticated. The NEAT feature is now enhanced to block the supplicant port during authentication, to ensure authentication completes.

  Use the **dot1x supplicant controlled transient** global configuration command to *control* access to the supplicant port during authentication. Use the **no** form of this command to *provide* access to the supplicant port during the authentication period.

Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release (after the first release) required to support the major features of the Catalyst Blade Switch 3120 for HP. Features not listed are supported in all releases.

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Blade Switch Support
Auto-QoS enhancements	12.2(55)SE	3120
Port ACL improvements	12.2(55)SE	3120
CDP location enhancements	12.2(55)SE	3120
Multi-authentication with VLAN assignment	12.2(55)SE	3120
Cisco TrustSec	12.2(55)SE	3120
MAC replace to end a session when a host disconnects from a port.	12.2(55)SE	3120
Full QoS support for IPv6 traffic.	12.2(52)SE	3120
Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications.	12.2(52)SE	3120
Support for IP source guard on static hosts.	12.2(52)SE	3120
RADIUS Change of Authorization (CoA)	12.2(52)SE	3120
IEEE 802.1x User Distribution	12.2(52)SE	3120
Critical VLAN with multiple-host authentication	12.2(52)SE	3120
Customizable web authentication enhancement	12.2(52)SE	3120

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Blade Switch Support
NEAT to change the port host mode and to apply a standard port configuration on the authenticator switch port	12.2(52)SE	3120
VLAN-ID based MAC authentication	12.2(52)SE	3120
MAC move	12.2(52)SE	3120
Support for including a hostname in the option 12 field of DHCPDISCOVER packets	12.2(52)SE	3120
DHCP snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE	3120
Support for VTP version 3.	12.2(52)SE	3120
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE	3120
Network Edge Access Topology (NEAT) with 802.1x	12.2(50)SE	3120
IEEE 802.1x with open access	12.2(50)SE	3120
IEEE 802.1x authentication with downloadable ACLs and redirect URLs	12.2(50)SE	3120
Flexible-authentication sequencing of authentication methods	12.2(50)SE	3120
Multiple-user authentication on an 802.1x-enabled port.	12.2(50)SE	3120
Cisco EnergyWise	12.2(50)SE	3120
Wired location service	12.2(50)SE	3120
Intermediate System-to-Intermediate System (IS-IS) routing	12.2(50)SE	3120
Stack troubleshooting enhancements	12.2(50)SE	3120
CPU utilization threshold trap	12.2(50)SE	3120
Embedded Event Manager Version 2.4	12.2(50)SE	3120
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling	12.2(50)SE	3120
RADIUS server load balancing	12.2(50)SE	3120
Auto Smartports Cisco-default and user-defined macros	12.2(50)SE	3120
Support for IPv6 features in the IP base and IP services feature sets	12.2(50)SE	3120
Voice aware IEEE 802.1x and MAC authentication bypass (MAB) security violation	12.2(46)SE	3120
Local web authentication banner	12.2(46)SE	3120
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3120
Disabling MAC address learning on a VLAN	12.2(46)SE	3120
PAgP Interaction with Virtual Switches and Dual-Active Detection, also referred to as enhanced PAgP	12.2(46)SE	3120
Support for rehosting a software license and for using an embedded evaluation software license	12.2(46)SE	3120
DHCP server port-based address allocation for the preassignment of an IP address to a switch port	12.2(46)SE	3120
HSRP for IPv6	12.2(46)SE	3120

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Blade Switch Support
DHCP for IPv6 relay, client, server address assignment and prefix delegation	12.2(46)SE	3120
IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router.	12.2(46)SE	3120
Generic message authentication support with the SSH Protocol and compliance with RFC 4256.	12.2(46)SE	3120

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.

Cisco IOS Limitations

Access Control List

- The Cisco Catalyst 3120 for HP Blade Switch has 964 TCAM entries available for ACLs in the default and routing SDM templates instead of the 1024 entries that are available on the Catalyst 3560 and Catalyst 3750 switches.

  There is no workaround. (CSCse33114)

- When a MAC access list is used to block packets from a specific source MAC address, that MAC address is entered in the switch MAC-address table.

  The workaround is to block traffic from the specific MAC address by using the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command. (CSCse73823)

Address Resolution Protocol

- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem. (CSCse06827))

Cisco X2 Transceiver Modules and SFP Modules

- Cisco X2-10GB-LR transceiver modules with a version identification number lower than V03 might show intermittent frame check sequence (FCS) errors or be ejected from the switch during periods of operational shock greater than 50 g. There is no workaround. (CSCse14048)
- Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number before V03 might intermittently fail. The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)
- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber). Use one of these workarounds:
  - Allow space between the switches when installing them.
  - In a switch stack, plan the SFP module and cable installation so that uplinks in adjacent stack members are not all in use.
  - Use a long, small screwdriver to access the latch, and then remove the SFP module and cable. (CSCsd57938)
- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based on IEEE 802.3ae. (CSCsd47344)

Configuration

- If a half-duplex port running at 10 Mb/s receives frames with Inter-Packet Gap (IPG) that do not conform to Ethernet specifications, the switch might stop sending packets.

  There is no workaround. (CSCec74610)
- When an excessive number (more than 100 packets per second) of Address Resolution Protocol (ARP) packets are sent to a Network Admission Control (NAC) Layer 2 IP-configured member port, a switch might display a message similar to this:

  ```
  PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism: type 0, class
  51, max_msg 128, total throttled 984323
  -Traceback= 6625EC 5DB4C0 5DAA98 55CA80 A2F2E0 A268D8
  ```

  No workaround is necessary. Under normal conditions, the switch generates this notification when snooping the next ARP packet. (CSCse47548)

- When there is a VLAN with protected ports configured in fallback bridge group, packets might not be forwarded between the protected ports.

  The workaround is to not configure VLANs with protected ports as part of a fallback bridge group. (CSCsg40322)

  When a switch port configuration is set at 10 Mb/s half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the **show controller ethernet-controller** or the **show interfaces** privileged EXEC commands.

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)

- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port.(CSCsi26392)

- The bootloader label is incorrect and displays “CISCO DEVELOPMENT TEST VERSION.” However, the actual bootloader software is the correct version with the correct functionality.

  There is no workaround. It does not impact functionality. (CSCta72141)

EtherChannel

- In an EtherChannel running Link Aggregation Control Protocol (LACP), the ports might be put in the suspended or error-disabled state after a stack partitions or a member switch reloads. This occurs when

  – The EtherChannel is a cross-stack EtherChannel with a switch stack at one or both ends.

  – The switch stack partitions because a member reloads. The EtherChannel is divided between the two partitioned stacks, each with a stack master.

  The EtherChannel ports are put in the suspended state because each partitioned stack sends LACP packets with different LACP Link Aggregation IDs (the system IDs are different). The ports that receive the packets detect the incompatibility and shut down some of the ports. Use one of these workarounds for ports in this error-disabled state:

  – Enable the switch to recover from the error-disabled state.

  – Enter the **shutdown** and the **no shutdown** interface configuration commands to enable the port.

  The EtherChannel ports are put in the error-disabled state because the switches in the partitioned stacks send STP BPDUs. The switch or stack at the other end of the EtherChannel receiving the multiple BPDUs with different source MAC addresses detects an EtherChannel misconfiguration.

  After the partitioned stacks merge, ports in the suspended state should automatically recover. (CSCse33842)

- When a switch stack is configured with a cross-stack EtherChannel, it might transmit duplicate packets across the EtherChannel when a physical port in the EtherChannel has a link-up or link-down event. This can occur for a few milliseconds while the switch stack adjusts the EtherChannel for the new set of active physical ports and can happen when the cross-stack EtherChannel is configured with either mode ON or LACP. This problem might not occur with all link-up or link-down events.

  No workaround is necessary. The problem corrects itself after the link-up or link-down event. (CSCse75508)

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

```
15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
(ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
4CEB50 859DF4 A7BF28 A98260 882658 879A58
```

  There is no workaround. (CSCsh12472)

HSRP

- When the switch stack is in the HSRP active state and a master changeover occurs, you cannot ping the stack by using an HSRP virtual IP address.

  There is no workaround. (CSCth00938)

IEEE 802.1x Authentication

- If a supplicant using a Marvel Yukon network interface card (NIC) is connected to an IEEE 802.1x-authorized port in multihost mode, the extra MAC address of 0c00.0000.0000 appears in the MAC address table.

  Use one of these workarounds (CSCsd90495):

  - Configure the port for single-host mode to prevent the extra MAC address from appearing in the MAC address table.
  - Replace the NIC with a new card.

- When MAC authentication bypass is configured to use Extensible Authentication Protocol (EAP) for authorization and critical authentication is configured to assign a critical port to an access VLAN:

  - If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.
  - If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.

  Use one of these workarounds (CSCse04534):

  - Configure MAC authentication bypass to not use EAP.
  - Define your network access profiles to not use MAC authentication bypass. For more information, see the Cisco Access Control Server (ACS) documentation.

- When IEEE 802.1x authentication with VLAN assignment is enabled, a CPUHOG message might appear if the switch is authenticating supplicants in a switch stack.

  The workaround is not use the VLAN assignment option. (CSCse22791)

Multicasting

- Multicast packets with a time-to-live (TTL) value of 0 or 1 are flooded in the incoming VLAN when all of these conditions are met:

  - Multicast routing is enabled in the VLAN.
  - The source IP address of the packet belongs to the directly connected network.
  - The TTL value is either 0 or 1.

The workaround is to not generate multicast packets with a TTL value of 0 or 1, or disable multicast routing in the VLAN. (CSCeh21660)

- Multicast packets denied by the multicast boundary access list are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the multicast packet belongs to a directly connected network.
  - The packet is denied by the IP multicast boundary access-list configured on the VLAN.

  There is no workaround. (CSCei08359)
- Reverse path forwarding (RPF) failed multicast traffic might cause a flood of Protocol Independent Multicast (PIM) messages in the VLAN when a packet source IP address is not reachable.

  The workaround is to not send RPF-failed multicast traffic, or make sure that the source IP address of the RPF-failed packet is reachable. (CSCsd28944)
- If the **clear ip mroute** privileged EXEC command is used when multicast packets are present, it might cause temporary flooding of incoming multicast traffic in the VLAN.

  There is no workaround. (CSCsd45753)
- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)
- When you configure the IGMP snooping throttle limit by using the **ip igmp max-groups** *number* interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number when all of these conditions are true:
  - The port-channel is configured with member ports across different switches in the stack.
  - One of the member switches reloads.
  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.

  The workaround is to disable the IGMP snooping throttle limit by using the **no ip igmp max-groups** *number* interface configuration command and then to reconfigure the same limit again. (CSCse39909)

Quality of Service (QoS)

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.

  There is no workaround. (CSCeh18677)
- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)
- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)

- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)

- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes. There is no workaround. (CSCsg79627)

- If QoS is enabled on a switch and the switch has a high volume of incoming packets with a maximum transmission unit (MTU) size greater than 1512 bytes, the switch might reload.

  Use one of these workarounds:

  - Use the default buffer size.
  - Use the **mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* global configuration command to allocate the buffer size. The buffer space for each queue must be at least 10 percent. (CSCsx69718)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

RADIUS

RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

There is no workaround. (CSCta05071)

Routing

- The switch stack might reload if the switch runs with this configuration for several hours, depleting the switch memory and causing the switch to fail:
  - The switch has 400 Open Shortest Path First (OSPF) neighbors.
  - The switch has thousands of OSPF routes.

  The workaround is to reduce the number of OSPF neighbors to 200 or less. (CSCse65252)

- When the PBR is enabled and QoS is enabled with DSCP settings, the CPU utilization might be high if traffic is sent to unknown destinations.

  The workaround is to not send traffic to unknown destinations. (CSCse97660)

SPAN and RSPAN

- When egress SPAN is running on a 10-Gigabit Ethernet port, only about 12 percent of the egress traffic is monitored.

  There is no workaround. This is a hardware limitation. (CSCei10129)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

Stacking

- When using the **logging console** global configuration command, low-level messages appear on both the stack master and the stack member consoles.

  The workaround is to use the **logging monitor** global configuration command to set the severity level to block the low-level messages on the stack member consoles. (CSCsd79037)

- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master, the new member might not get the latest running configuration and might not operate properly.

  The workaround is to reboot the new member switch. Use the **remote command all show run** privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)

- When the flash memory of a stack member is almost full, it might take longer to start up than other member switches. This might cause that switch to miss the stack-master election window. As a result, the switch might fail to become the stack master even though it has the highest priority.

  The workaround is to delete files in the flash memory to create more free space. (CSCsg30073)

- The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:
  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.

  You can use one of these workarounds:
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
  - Remove and reconfigure the VLAN. (CSCsi26444)

- When you use the **switch renumber** global configuration command to renumber a member switch in a switch stack and then reload the switch, the internal server-facing ports do not have the required default of **spanning-tree portfast** enabled.

  The workaround is to apply the switch provision configuration before you reboot the switch. Enter both the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* and the **switch** *stack-member-number* **provision** *type* global configuration commands, and reload the switch. (CSCsl63862)

- If you enter the **show tech-support** privileged EXEC command after you enter the **remote command** {**all** | *stack-member-number*} privileged EXEC command, the complete output does not appear.

  The workaround is to use the **session** *stack-member-number* privileged EXEC command. (CSCsz38090)

VLANs

- When the domain is authorized in the guest VLAN on a member switch port without link loss and an Extensible Authentication Protocol over LAN (EAPOL) is sent to an IEEE 802.1x supplicant to authenticate, the authentication fails. This problem happens intermittently with certain stacking configurations and only occurs on the member switches.

  The workaround is to enter the **shut** and **no shut** interface configuration commands on the port to reset the authentication status. (CSCsf98557)

Device Manager Limitations

- 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 start.

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

- If you launch the device manager from a Firefox web browser, an invalid certificate alert appears. If you launch the device manager from an Internet Explorer 7.0 browser, a certificate error appears.

  The workaround when using Firefox is to either temporarily or permanently accept the certificate. If you temporarily accept the certificate, close and then reopen the Firefox browser window. If you permanently accept the certificate, delete the certificate, and then close and restart Firefox:

  – If you are using Firefox version 1.5, choose **Tools > Options > Advanced > Security > View Certificates > Web Sites**, select the certificate, and click **Delete**.

  – If you are using Firefox version 2.0, choose **Tools > Options > Advanced > Encryption > View Certificates > Web Sites**, select the certificate, and click **Delete**.

  The workaround when using Internet Explorer is to click **Click here for Options** in the warning message, and click **Display Blocked Content**. Close the browser window, and launch a new session. (CSCsk80229)

Important Notes

Cisco IOS Notes

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.

- 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)EX1 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 interfaces 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

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- We recommend this browser setting to reduce the time needed to display the device manager from Microsoft Internet Explorer.

  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** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**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.

Open Caveats

- CSCth94904

  An internal switch port is down when one of these HP Flex 10-Gigabit Ethernet network interface cards (NICs) is up:

  – Flex 522m Mezz

  – Flex 542m Mezz

  – Flex 552m Mezz

  The workaround is to use the **speed nonegotiate** interface configuration command on the internal port.

- CSCto57605

  If the Dynamic Trunking Protocol (DTP) is set to speed nonegotiate for two switches that interface each other, and the speed/duplex is configured as full/1000, the speed/duplex configuration of one of the switches changes to auto/auto when the switch is restarted. The port channel becomes incompatible and the second switch's operation is suspended. This problem applies only to the 1000BASE-LX interface.

  The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command.

- CSCtx37129

  If you enter the **shutdown** interface configuration command on the the Fast Ethernet 0 router interface and VLAN 1 client switch interface, and then restart the master switch, the shutdown status of these two interfaces are not shown correctly. If you check their status with the **show running-config** privileged EXEC command, these interfaces are shown as up..

  There is no workaround.

- CSCtx73953

  A port that is programatically configured with auth-default ACL does not allow any traffic on the switch except DHCP traffic. If the configurations on the interface are cleared and the interface is restarted, the auth-default ACL configuration remains and the problem persists.

  There is no workaround.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 12.2(55)SE5

- CSCsy43147

  During a Telnet session, the router crashes when the TACACS+ server is configured or unconfigured (**tacacs-server host** command) using the **single-connection** keyword.

  The workaround is to not use the **single-connection** keyword.

- CSCtb35715

  When you enter the **show running-config** interface configuration command, IP Service Level Agreement notifications are shown as enabled even when you have not enabled this configuration using the **ip sla enable reaction-alerts** interface configuration command.

  There is no workaround.

- CSCtc18841

  If local proxy Address Resolution Protocol (ARP) is configured on the VLAN interface, the ARP entry for the Hot Standby Router Protocol (HSRP) enters into an incomplete state.

  The workaround is to remove the proxy ARP feature on the VLAN interface (by using the **no ip local-proxy-arp** interface configuration command) and restart the interface.

- CSCtg38468

  When AAA authorization is used with TACACS+, an error is displayed if the banner message (**banner exec** global configuration command) starts with a blank character.

  The workaround is to not start the banner message with a blank character.

- CSCth00398

  If the **no vtp** VLAN configuration command is used on a port that receives VTP updates, the switch does not process Layer 2 control traffic (STP and CDP) after some time.

  The workaround is to configure VTP on the port or to not use the **no vtp** command.

- CSCtj22354

  The switch fails when LLDP data units with Type Length Value (TLV) of more than 10 management addresses (MA) are received.

  The workaround is to disable the sending of LLDP MA TLVs on peer hosts.

- CSCtj88307

  When you enter the **default interface**, **switchport**, or **no switchport** interface configuration command on the switch, this message appears:

  ```
  EMAC phy access error, port 0, retrying......
  ```

  There is no workaround.

- CSCtj89743

  CPU usage is high when a device connected to the switch is accessed using the *https://IP_address* command on the router.

  The workaround is to reload the device.

- CSCtn10697

  The switch crashes when DCHP snooping is enabled with value 125 and an offer packet is received.

  There is no workaround.

- CSCto72927

  If a Tcl policy is copied to the router, the router fails when an event manager policy is configured.

  There is no workaround.

- CSCtq09233

  If a CLI configuration text file is copied from a Windows system to the switch, a space is appended to the end of the macro description command when the file is read from the flash of the switch. This leads to errors resulting in high CPU utilization on the switch. Another possible issue is that the macro is not removed when the link goes down or the connected device is removed from the switch.

  The workaround is to copy the configuration file from a non-Windows system (like UNIX or Linux) or convert the file to an appropriate UNIX format before copying.

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts34688

  The switch crashes due to the "HACL Acl Manager" memory fragmentation when a large access control list (ACL) is modified.

- CSCts54282

  A memory leak occurs when a Switch Virtual Interface (SVI) is configured and an external management port is disabled on the Advanced Management Module (AMM).

  There is no workaround.

- CSCts58073

  A threshold violation error message is displayed when a X2-10GB-LR module is installed on the switch (with or without a fiber cable). An example error message is:

  ```
  SFF8472-5-THRESHOLD_VIOLATION: Te1/0/1: Voltage low alarm; Operating value: 0.00 V,
  Threshold value: 2.96 V
  ```

  There is no workaround.

- CSCts75641

  Routing Information Protocol (RIP) Version 2 packets egressing an 801.1Q tunnel interface are triplicated.

  There is no workaround.

- CSCtt16051

  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt37202

  If a client switch is authorized using MAC Authentication Bypass (MAB), and then by using the 802.1x standard and dynamic VLAN assignment, the MAC address of the switch is not updated in the MAC address table of slave switches.

  The workaround is to not use both the 802.1x and dynamic VLAN assignment configurations for the client switch.

- CSCtu17483

  The switch crashes when an IP phone that uses LLDP and authenticates itself using MAC Authentication Bypass (MAB) or 802.1x is physically disconnected and reconnected to the switch port.

  The workaround is to remove the **aaa authorization network default group SG-PBA** global configuration command.

Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- CSCta85026

  The Dynamic Host Configuration Protocol (DHCP) CLI does not accept white spaces in raw ASCII option in the DHCP pool configuration submode. This issue is seen in Cisco IOS Release 12.4(24)T1 and later.

  There is no workaround.

- CSCtg11547

  In a VPN Routing and Forwarding (VRF) aware setup, messages are not sent to the syslog server. This issue applies to Cisco IOS Release 12.2(53)SE and 12.2(53)SE1. This situation does not occur if system logging is configured in the global table.

  This problem has been corrected.

- CSCth03648

  When two traps are generated by two separate processes, the switch fails if one process is suspended while the other process updates some variables used by the first process.

  The workaround is to disable all SNMP traps.

- CSCth87458

  A memory leak occurs in the SSH process, and user authentication is required.

  The workaround is to allow SSH connections only from trusted hosts.

- CSCti37197

  If a tunnel interface is configured with Cisco Discovery Protocol (CDP), the switch fails when it receives a CDP packet.

  The workaround is to disable CDP on the interface by using the **no cdp enable** interface configuration command.

- CSCtj56719

  The switch fails when the Differentiated Services Code Point (DSCP) mutation name is longer than 25 characters.

  The workaround is to configure DSCP mutation names with fewer than 25 characters.

- CSCtj83964

  On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.

  The workaround is to enter the **clear ip route** privileged EXEC command or reconfigure PIM and SSM after a reload.

- CSCtk00846

  If Auto Smartports macros are configured, access points with the AIR-CAP prefix are not detected.

  The workaround is to manually configure the access point port.

- CSCtl51859

  Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.

  The workaround is to disable IPv6 MLD snooping on the switch.

- CSCtl60151

  The switch sometimes reloads after a CPU overload, regardless of the process that is overloading the CPU.

  This problem has been corrected.

- CSCtn11259

  If a switch stack is configured with the **stack-mac persistent timer** *value* interface configuration command, the switch virtual interface (SVI) should remain in shutdown mode during a switchover. In this case, the SVI is in up mode.

  The workaround is to specify the timer value to be long enough so that the stack's MAC address is not changed.

- CSCto67688

  If a member switch does not have an access control list (ACL) and is running an Enforcement Policy Module (EPM) session, the client on that interface is re-authorized each time that the switch reloads.

  The workaround is to configure an ACL on the interface.

- CSCtr79386

  The switch fails when DHCP snooping is configured and packet data traffic is excessive. The traffic exhausts the I/O memory and triggers the switch to crash.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(55)SE3

- CSCtg71149

  When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, indicated by the appearance of `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.

  The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

  - Enter the **shutdown** interface configuration command on each member port.
  - Enter the shutdown command on the port-channel interface.
  - Enter the **no shutdown** command on each member port.
  - Enter the **no shutdown** command on the port-channel interface.

- CSCtn18139

  When the **show spanning-tree vlan** *VLAN* **interface fastethernet 0** command is entered, the switch restarts.

  The FastEthernet 0 interface is a management interface that does not run Spanning Tree Protocol (STP). Do not run **show spanning-tree** commands for management interfaces.

- CSCto55124

  When a member switch port security is used with port-based dot1x authentication and the switch MAC address is sticky, a connected device authenticates itself. Its MAC address is added as sticky in the switch configuration and in the port security tables of the stack switches. When the switch is

shut down, the device MAC address is removed from the master switch, but it is retained in the member switch security tables. When the interface is re-enabled, the device MAC address is restored to the master switch configuration.

The workaround is to use port security without dot1x authentication.

Caveats Resolved in Cisco IOS Release 12.2(55)SE2 and Earlier

- CSCsg28558

  Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to install because of a size discrepancy.

  The workaround is to use modules with a version identification number of V03 or later.

- CSCsg91027

  When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

  High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:

  Disable logging to the console.

  Rate-limit logging messages to the console.

  Remove the **logging event spanning-tree** interface configuration command from the interfaces.

- CSCsu31853

  The buffer space of a switch running TCP applications is full while the TCP sessions are in the TIME_WAIT state. Buffer space becomes available after the TCP session the closed.

  There is no workaround.

- CSCsz18634

  On a switch running Cisco IOS release 12.2(46)SE, the output of the **show interfaces** privileged EXEC command shows 0 packets for port channel input and output rates.

  The workaround is to reload the switch by entering the **reload** privileged EXEC command.

- CSCtb08823

  SNMP requests on the stpxRSTPPortRoleTable object only return information for the stack master.

  There is no workaround.

- CSCtb25230

  When a switch stack is configured with DHCP snooping enabled on the host VLAN, hosts connected to the stack master receive bootp packets, but the a packet might not be forwarded to the end hosts connected to stack member switches. The behavior depends on which interface in the stack received the packet.

  The workaround is to disable DHCP snooping for the affected VLAN.

- CSCtb58779

  When a switch is low on memory (less than 256 MB), it can reload and display a SYS-2-WATCHDOG error.

  There is no workaround. Enter the **show memory debug leak** privileged EXEC command to check for signs of a memory leak and address these symptoms.

- CSCtc02635

  On switches running Cisco IOS release 12.2(50)SE3 running MAC authentication bypass with multidomain authentication (MDA, IP phones connected to a port might not be able to regain network connectivity in the VOICE domain if the session times out and all RADIUS servers are unreachable.

  There is no workaround.

- CSCtc57809

  Switches running Cisco IOS Release 12.2(52)SE might reload after you enter the **no mac address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id* global configuration command if the interface is up and the MAC address was dynamically learned before it was changed to static.

  Use one of these workarounds:

  - Clear the dynamic MAC address table when configuring static MAC addresses as in this example:

    ```
    Switch(config)# no mac address-table learning vlan vlan_id
    Switch(config)# clear mac-address-table dynamic address mac_address
    Switch(config)# mac address-table static mac_address vlan vlan_id interface interface_id
    Switch(config)# mac address-table learning vlan vlan_id
    ```

  - Downgrade to Cisco IOS Release 12.2(50)SE.
  - Upgrade to Cisco IOS Release 12.2(53)SE if available.

- CSCtc77969

  When PAgP or LACP EtherChannels are configured on a switch and the stack reloads, entering a **show interface** or **show etherchannel summary** privileged EXEC command when the stack comes up can cause the console to lock up.

  There is no workaround.

- CSCte00827

  When a port that is configured for Switched Port Analyzer (SPAN) goes up and down, a memory leak occurs in the ‘hpm main’ process.

  There is no workaround.

- CSCtd02006

  After a 10-Gigabit Ethernet interface in an X2-10GB-SR module is down and the switch is restarted, the show inventory command output shows the module as not present.

  The workaround is to reinstall the X2-10GB-SR module or to restart the switch.

- CSCtd29049

  A switch that has at least one trunk port configured might fail when you configure more than 950 VLANS by using the **vlan** vlan-id global configuration command.

  There is no workaround.

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte72365

  After a software upgrade from Cisco IOS Release 12.2(52)SE to Cisco IOS Release 12.2(53)SE, EIGRP hello packets are flooded on access ports belonging to another subnet. The same result occurs when you initiate ping requests to the broadcast address of other subnets. This results in *Not on common subnet* errors on the other side of the link.

  The workaround is to downgrade to 12.2(52)SE

- CSCte94620

  After you apply an ACL, these messages appear:

  ```
  %IPACCESS-4-INVALIDACL: Invalid ACL field: Acl number is 0
  %IPACCESS-4-INVALIDACL: Invalid ACL field: Acl type is 145
  ```

  There is no workaround.

- CSCte99650

  A Cisco Catalyst switch can report abnormal temperatures even though the output of the **show environment all** user EXEC or privileged EXEC command shows that the temperatures are within acceptable limits.

  This is an example of the system messages:

  ```
  Dec 25 19:03:57.463 AEST: %PLATFORM_ENV-1-TEMP: Abnormal temperature detected
  Jan  2 04:04:46.600 AEST: %PLATFORM_ENV-1-TEMP: Abnormal temperature detected
  Jan  7 06:33:36.067 AEST: %PLATFORM_ENV-1-TEMP: Abnormal temperature detected
  ```

  This is an example of the output of the **show environment all** command:

  ```
  Switch# show environment all
  TEMPERATURE is OK
  Temperature Value: 39 Degree Celsius
  Temperature State: GREEN
  Yellow Threshold : 80 Degree Celsius
  Red Threshold    : 90 Degree Celsius
  ```

  There is no workaround.

- CSCtf19991

  If the RADIUS authentication server is unavailable and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the connected port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. After the server is available, the client is not reinitialized and moved out of the critical VLAN.

  There is no workaround.

- CSCtf33948

  A PC in 802.1x or multidomain authentication (MDA) mode is connected to an IP phone and connected to a MDA-enabled switch port. After the PC and phone are authenticated on the port, the PC is down. The port does not automatically reauthenticate the PC.

  There is no workaround.

- CSCtf78276

  A switch running Cisco IOS Release 12.2(53)SE1 stops when IEEE 802.1x authentication is enabled.

  The workaround is to apply a VLAN that the RADIUS server assigned to the switch.

- CSCtg26941

  Multidomain authentication (MDA) with guest VLAN or MAC authentication bypass (MAB) as a fallback method is enabled on a switch running Cisco IOS Release 12.2(53)SE. When a non-802.1x client is connected to a IP phone and the phone connected to a switch port shuts down and then restarts, the client MAC address status is *drop* in the MAC address table. It takes 5 minutes for the client to access the network.

  The workaround is to use another software release, such as Cisco IOS Release 12.2(44)SE2.

- CSCtg47738

  This error message is displayed after copying a configuration file to the running configuration file fails:

  ```
  %Error opening system:/running-config (No such file or directory)
  ```

  The output of the **dir system:/** EXEC command also does not show a running configuration file.

  The workaround is to reload the switch.

- CSCth18118

  When VTP pruning is enabled in a VTP domain, the switch in VTP server mode sends advertisements to neighboring switches. If the VTP and VLAN configuration for neighboring ports is not updated, VLANs on those ports can be pruned, causing a network traffic outage.

  The workaround is to disable VTP pruning.

- CSCth88306

  This message appears after inserting the CVR-X2-SFP converter module and the X2-10GB-SR transceiver modules in the10-Gigabit slots of the Catalyst 3750-E and 3560-E switches:

  ```
  %GBIC_SECURITY_CRYPT-4-VN_DATA_CRC_ERROR: GBIC in port Te1/0/1 has bad crc
  ```

  There is no workaround.

- CSCti04980

  After you upgrade the switch software to Cisco IOS Release 12.2(55)SE, enhanced auto-QoS commands are generated when

  – auto-QoS is enabled on an interface

  and

  – **mls qos** command is not enabled on the switch

  If the **mls qos** command was already enabled on the switch, enhanced auto-QoS commands are generated only when you configure one of these commands:

  – **auto qos classify** [**police**]

  – **auto qos trust** {**cos** | **dscp**}

  – **auto qos video** {**cts** | **ip-camera**}

  Cisco IOS Release 12.2(55)SE supports implicit and explicit migration to enhanced auto-QoS configurations.

  Implicit migration to enhanced auto-QoS occurs on a switch running legacy auto-QoS when you configure the **auto qos video**, **auto qos trust**, or **auto qos classify** command on an interface. Global and interface configurations on the switch migrate to the enhanced video or trust auto-QoS configurations.

  Explicit migration to enhanced auto-QoS occurs on a switch when you enable the **auto qos srnd4** global configuration command. You can configure the [**no**] form of this commandafter you remove auto-QoS functionality from all switch interfaces.

- CSCtj03875

  When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.

  There is no workaround.

- CSCtj86299

  If a static MAC address entry is configured for an IP address in the global routing table, ping requests are sent through the global context, and replies are sent through Virtual Routing and Forwarding (VRF). This is a VRF leak.

  The workaround is to remove the static MAC address entry.

Documentation Updates

Updates to the Software Configuration Guide

In the "Configuring RIP for IPv6" section in the "Configuring IPv6 Unicast Routing" chapter, the task table is incorrect. This is the correct table:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 router rip** *name*	Configure an IPv6 RIP routing process, and enter router configuration mode for the process.
Step 3	**maximum-paths** *number-paths*	(Optional) Define the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 32, and the default is 16 routes.
Step 4	**exit**	Return to global configuration mode.
Step 5	**interface** *interface-id*	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 6	**ipv6 rip** *name* **enable**	Enable the specified IPv6 RIP routing process on the interface.
Step 7	**ipv6 rip** *name* **default-information** {**only** | **originate**}	(Optional) Originate the IPv6 default route (::/0) into the RIP routing process updates sent from the specified interface. **Note** To avoid routing loops after the IPv6 default route (::/0) is originated from any interface, the routing process ignores all default routes received on any interface. • **only**—Select to originate the default route, but suppress all other routes in the updates sent on this interface. • **originate**—Select to originate the default route in addition to all other routes in the updates sent on this interface.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show ipv6 rip** [*name*] [**database**] [**next-hops**] or **show ipv6 route rip** [*updated*]	Display information about IPv6 RIP processes. Display the contents of the IPv6 routing table.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Updates to the Switch Getting Started Guide

When you launch Express Setup, you are prompted for the switch password. Enter the default password, *cisco*. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, *cisco*.

Updates for the System Message Guide

New System Messages

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

Explanation A host on the interface attempted to gain access to the network or attempted an authentication. The interface mode does not support the number of hosts that are attached to the interface. This is a security violation, and the interface has been error-disabled. The first [chars] is the interface, [enet] is the Ethernet address of the host, and the second [chars] is the session ID.

Recommended Action Make sure that the interface is configured to support the number of hosts that are attached to it. Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command to restart the interface.

Error Message `AUTHMGR-5-VLANASSIGN: VLAN [dec] assigned to Interface [chars] AuditSessionID [chars]`

Explanation A VLAN was assigned. [dec] is the VLAN ID, the first [chars] is the interface, and the second [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-FAILOVER: Failing over from [chars] for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation The authorization manager is failing over from the current authentication method to another method. The first [chars] is the current authentication method, the second [chars] is the client ID, the third [chars] is the interface, and the fourth [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation All available authentication methods have been tried for the client, but authentication has failed. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required. If local authorization has been configured, the port will be authorized based on the local authorization method. Otherwise, authentication will restart according to the configured reauthentication period.

Error Message `AUTHMGR-7-RESULT: Authentication result [chars] from [chars] for client [chars] on Interface [chars] AuditSessionID [chars]`

Explanation The results of the authentication. The first [chars] is the status of the authentication, the second [chars] is the authentication method, the third [chars] is the client ID, the fourth [chars] is the interface, and the fifth [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation The authentication was unsuccessful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action. AuditSessionID [chars]`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication. [chars] is the session ID.

Recommended Action Reduce other system activity to reduce memory demands.

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was successful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars] AuditSessionID [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. This message might appear if IEEE 802.1x is enabled. [enet] is the client MAC address, the first [chars] is the interface, and the second [chars] is the session ID.

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

Error Message `EPM-6-AUTH_ACL: POLICY [chars]| EVENT [chars]`

Explanation The switch has sent or received a download request for a downloadable ACL (dACL). The first [chars] is the dACL policy? The second [chars] is the event.

Recommended Action No action is required.

Error Message `HARDWARE-3-ASICNUM_ERROR: [traceback] Port-ASIC number [dec] is invalid`

Explanation The port ASIC number is invalid. [dec] is the port ASIC number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `HARDWARE-3-PORTNUM_ERROR: [traceback] port number [dec] is invalid`

Explanation The port number is out of range. [dec] is the port number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `HULC_LICENSE-1-LICENSE_REGISTER_FAILED: [chars] - rc = [dec]`

Explanation The licensing initialization failed. [chars] explains what part of the license registration failed, and [dec] is the type of license initialization error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `IFMGR-3-IFINDEX_PERSIST_ENTRY_CORRUPT: [chars] seems to be corrupted. Trying to read [dec] size`

Explanation The ifIndex table is corrupted. [chars] is the path to the IfIndex file, and [dec] is the number of bytes that was being read from the ifIndex table when the corruption was detected.

Recommended Action Delete the ifindex table.

Error Message `IFMGR-3-INVALID_PERSISTENT_DATA: Invalid persistent data`

Explanation The interface manager attempts to write invalid persistent data.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `ILET-1-AUTHENTICATION_FAIL: This Switch may not have been manufactured by Cisco or with Cisco's authorization. This product may contain software that was copied in violation of Cisco's license terms. If your use of this product is the cause of a support issue, Cisco may deny operation of the product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco's Technical Assistance Center for more information.`

Explanation A license authentication failure occurred for the switch.

Recommended Action Contact your Cisco sales representative for assistance.

Error Message `ILET-1-DEVICE_AUTHENTICATION_FAIL: The [chars] inserted in this switch may not have been manufactured by Cisco or with Cisco's authorization. If your use of this product is the cause of a support issue, Cisco may deny operation of the product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco's Technical Assistance Center for more information.`

Explanation A license authentication failure occurred for a component that was inserted in the switch. [chars] is the component.

Error Message `SCHED-3-UNEXPECTEDEVENT: [traceback] [process information] Process received unknown event (maj [hex], min [hex])`

Explanation A process did not handle an event. The first [hex] is the major event number, and the second [hex] is the minor event number, both of which allow you to identify the event that occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Recommended Action Contact your Cisco sales representative for assistance.

Modified System Messages

Error Message `DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation The authentication result was overridden. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a primary VLAN to an 802.1x port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Use a different VLAN.

Note This message applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a nonsecondary VLAN to a private VLAN host 802.1x port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the port mode so that it is no longer a PVLAN host port, or use a valid secondary VLAN.

Note This message applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure that the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

Note This message applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the port mode so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_MDA_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port AuditSessionID [chars]`

Explanation Multi-Domain Authentication (MDA) host mode cannot start when the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port session ID.

Recommended Action Change either the voice VLAN or the access VLAN on the interface so that they are not the same. MDA then starts.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Update the configuration to use a valid VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [chars] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the VLAN exists and is not shut down, or use another VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Attempt to assign VLAN [dec] to routed 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to a supplicant on a routed port, which is not allowed. [dec] is the VLAN ID, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Either disable the VLAN assignment, or change the port type to a nonrouted port.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_PROMISC_PORT: Attempt to assign VLAN [dec] to promiscuous 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to a promiscuous IEEE 802.1x port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the port mode so that it is no longer a promiscuous port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_RESERVED: Attempt to assign reserved VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is a reserved VLAN and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the seconds [chars] is the session ID.

Recommended Action Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_RSPAN: Attempt to assign RSPAN VLAN [dec] to 802.1x port [chars]. 802.1x is incompatible with RSPAN AuditSessionID [chars]`

Explanation Remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Either disable remote SPAN configuration on the VLAN, or disable IEEE 802.1x on all the ports in this VLAN.

Error Message `SPANTREE-2-BLOCK_BPDUGUARD_VP: Received BPDU on port [chars], vlan [dec] with BPDU Guard enabled. Disabling vlan.`

Explanation A BPDU was received on the interface and the VLAN specified in the error message. The spanning tree BPDU guard feature was enabled and configured to shut down the VLAN. As a result, the VLAN was placed in the error-disabled state. [chars] is the interface, and [dec] is the VLAN.

Recommended Action Either remove the device sending BPDUs, or disable the BPDU guard feature. The BPDU guard feature can be locally configured on the interface or globally configured on all ports that have Port Fast enabled. Re-enable the interface and vlan by entering the **clear errdisable** privileged EXEC command.

Deleted System Messages

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action.`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication.

Recommended Action Reduce other system activity to reduce memory demands.

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars]`

Explanation Authentication was successful. [chars] is the interface.

Recommended Action No action is required.

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. This message might appear if IEEE 802.1x is enabled. [enet] is the client MAC address, and [chars] is the interface.

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

Error Message `SW_VLAN-4-VTP_USER_NOTIFICATION: VTP protocol user notification: [chars].`

Explanation This message means that the VTP code encountered an unusual diagnostic situation. [chars] is a description of the situation.

Recommended Action Find out more about the error by using the s**how tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Related Documentation

These documents provide complete information about the Cisco Catalyst 3120 for HP Blade Switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6748/tsd_products_support_series_home.html

- *Cisco Catalyst Blade Switch 3000 Series for HP Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3000 Series for HP*

- *Release Notes for the Cisco Catalyst Blade Switch 3120 for HP*

Note Before you install, configure, or upgrade the switch module, see the release notes on Cisco.com for the latest information.

- *Cisco Catalyst Blade Switch 3120 for HP Software Configuration Guide*
- *Cisco Catalyst Blade Switch 3120 for HP Command Reference*
- *Cisco Catalyst Blade Switch 3120 for HP System Message Guide*
- *Cisco Software Activation Document for HP*
- These compatibility matrix documents are available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

For other information about related products, see these documents on Cisco.com:

- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Network Admission Control Software Configuration Guide*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.