Release Notes for Cisco Catalyst Blade Switch 3120 for HP, Cisco IOS Release 12.2(50)SE and Later

Revised October 21, 2010

Cisco IOS Release 12.2(50)SE and later 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(50)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 5.
- 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 5.

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

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438038

This software release is part of a special release of Cisco IOS software that is not released on the same maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

For the complete list of the Cisco Catalyst Blade Switch 3120 for HP documentation, see the "Related Documentation" section on page 43.

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

These sections provide information about this release:

System Requirements

The system requirements are described in these sections:

- Hardware Supported, page 2
- Device Manager System Requirements, page 4
- Cisco Network Assistant Compatibility, page 4

Hardware Supported

Table 1 lists the hardware supported on this release.

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 (supported only on the CBS3120X-S model)	X2-10GB-SR V02 or later X2-10GB-CX4 V03 or later X2-10GB-LRM V03 or later X2-10GB-LX4 V03 or later 10 Gigabit Ethernet X2 ZR optical modules	Cisco IOS Release 12.2(40)EX1 Cisco IOS Release 12.2(50)SE
Cisco TwinGig Converter Module	Dual SFP[2] X2 converter module to allow the switch to support SFP Gigabit Ethernet modules	Cisco IOS Release 12.2(40)EX1
SFP modules	1000BASE-LX/LH 1000BASE-SX 1000BASE-T SFP-10G-SR SFP-10G-LR	Cisco IOS Release 12.2(40)EX1 Cisco IOS Release 12.2(50)SE

[1] X2 module supported only on the CBS3120X-S model

[2] SFP = small form-factor pluggable

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

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

- Hardware Requirements, page 4
- Software Requirements, page 4

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, page 5
- Deciding Which Files to Use, page 5
- Upgrading a Switch by Using the Device Manager or Network Assistant, page 6
- Upgrading a Switch by Using the CLI, page 6
- Recovering from a Software Failure, page 7

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.

Table 3 lists the filenames for this software release.

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.122-50.SE5.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.122-50.SE5.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/products/sw/iosswrel/ps5187/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/12_2/configfun/command/reference/ffun_r.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. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=268438038

To download the universal software image files for a Cisco Catalyst Blade Switch 3120 for HP, click **Blade Switches > Cisco Catalyst Blade Switch 3000 Series for HP >**. To obtain authorization and to download the cryptographic software files, click **Cisco Catalyst Blade Switch 3000 Series for HP Cryptographic Software**.

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 Features

These sections describe the new supported hardware and the new and updated software features provided in this release:

- New Hardware Features, page 8
- New Software Features, page 8

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

These are the new software features for this release:

- Network Edge Access Topology (NEAT) with 802.1x switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- IEEE 802.1x with open access to allow a host to access the network before being authenticated.
- IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch.
- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.
- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.
- Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE).
- Intermediate System-to-Intermediate System (IS-IS) routing supports dynamic routing protocols for Connectionless Network Service (CLNS) networks (only with the IP services feature set).
- Stack troubleshooting enhancements.
- CPU utilization threshold trap monitors CPU utilization.
- Support for the Cisco IOS Configuration Engine, previously referred to as the Cisco IOS CNS agent.
- Support for Embedded Event Manager Version 2.4.
- LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.
- Support for up to 64 EtherChannels.
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Auto Smartports Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port.

- These IPv6 features are now supported in the IP services and IP base software licenses:

Feature	Releases Earlier Than Cisco IOS Release 12.2(50)SE	Cisco IOS Release 12.2(50)SE and Later
Access control lists (ACLs)	Advanced IP services	IP base
DHCP for IPv6 (DHCPv6) for the DCHP server, client, and relay device	Advanced IP services	IP base
Enhanced Interior Gateway Routing Protocol for IPv6 (EIGRPv6)	Advanced IP services	IP services
Hot Standby Router Protocol for IPv6 (HSRPv6)	Advanced IP services	IP services
Open Shortest Path First Version 3 (OSPFv3)	Advanced IP services	IP services
Routing Information Protocol (RIP)	Advanced IP services	IP base
Static routes	Advanced IP services	IP base

The advanced IP services software license is now end-of-sale (EOS) and end-of-life (EOL). For more information, see http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps7077/eol_c51_519629.html

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
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

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
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
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.

This section contains these limitations:

- Cisco IOS Limitations, page 10
- Device Manager Limitations, page 17

Cisco IOS Limitations

These limitations apply to the Cisco Catalyst Blade Switch 3120 for HP:

- Access Control List, page 11
- Address Resolution Protocol, page 11
- Cisco X2 Transceiver Modules and SFP Modules, page 11
- Configuration, page 12
- EtherChannel, page 13
- IEEE 802.1x Authentication, page 13

Access Control List

These are the access control list (ACL) limitations:

- 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

This is an Address Resolution Protocol limitation:

- 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

These are the Cisco X2 transceiver module and SFP module limitations:

- 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)
- Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to insert because of a dimensional tolerance discrepancy. The workaround is to use modules with a version identification number of V03 or later. (CSCsg28558)
- 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)
- Cisco GLC-GE-100FX SFP modules with a serial number between OPC0926xxxx and OPC0945xxxx might show intermittent *module not valid*, data, status, link-flapping, and FCS errors. The workaround is to use modules with serial numbers that are not in the specified range. (CSCsh59585)

- 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)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module. The workaround is to configure aggressive UDLD. (CSCsh70244).

Configuration

These are the configuration limitations:

- 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)

EtherChannel

These are the EtherChannel limitations:

- 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)

IEEE 802.1x Authentication

These are the IEEE 802.1x authentication limitations:

- 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

These are the multicasting limitations:

- 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)

QoS

These are the quality of service (QoS) limitations:

- 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)

Routing

These are the routing limitations:

- 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

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

- 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)
- 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 (CSCsg91027):
  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces.
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

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

VLANs

This is a VLAN limitation:

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)

Stacking

These are the switch stack limitations:

- 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)

- 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)

Device Manager Limitations

These are the 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

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

- Cisco IOS Notes, page 18
- Device Manager Notes, page 18

Cisco IOS Notes

These notes apply to Cisco IOS software:

- 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

These notes apply to the device manager:

- 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

- CSCsg67684

  When a cross-stack LACP EtherChannel has a maximum configuration, such as eight active and eight hot-standby ports, and there are multiple rapid sequential master failovers and stack rejoins that cause extreme stress, the port channel might not function as expected. Some ports might not join the EtherChannel, and traffic might be lost. You can detect the condition by using the **remote command all show etherchannel summary** privileged EXEC command.

  There is no workaround. The out-of-sync switches must be reloaded.

- CSCsi06399

  When a RIP network and IP address are configured on an interface, a traceback error occurs after you enter the **shutdown**, **no shutdown, switchport,** and **no switchport** interface configuration commands.

  The workaround is to configure the RIP network and the IP address after you configure the interface.

- CSCsi14303

  When booting a switch stack configured for IP source guard with port security and dynamic ARP inspection, a message similar to this might appear:

  ```
  SYS-2-LINKED: Bad enqueue of 2A3DE74 in queue 22881BC (l3a3-9) -Process=
  "Port-Security", ipl= 6, pid= 161 (l3a3-9) -Traceback= 119CC50 11D2264 9571E0 119B4E0
  95D41C 80DBD8 80E734 80B998 80AAD4 80B55C 9EB158 9E2544 (l3a3-9)
  ```

  There is no workaround. This message is only information; switch functionality is not affected.

- CSCsi26444

  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.

- CSCsi52914

  When you are configuring a SPAN session, this message might erroneously appear even when two source sessions are not configured:

  ```
  % Platform can support a maximum of 2 source sessions
  ```

  The workaround is to reboot the switch stack.

- CSCsi65551

  In certain situations during master switch failover, a VLAN that has been error disabled on a port might be re-enabled after the master switch failover, even though the port has not been configured for automatic recovery.

  There is no workaround.

- 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.

  The workaround is to configure routed IPv4 multicast and IPv6 unicast traffic in different switch ports.

- CSCsi73653

  After a stack-master failover, switch ports in the stack cannot detect new devices. This only affects new devices connected to the switch ports. Devices that were connected to active ports before the failover remain in a trusted state.

  There is no workaround.

- CSCsj22678

  A delay can occur when you remove an access control list (ACL) from a switch stack under these conditions:

  - A QoS, per-port policy map is attached to a large number of SVIs in the stack.
  - A per-VLAN QoS, per-port policer policy map is attached to a large number of switched virtual interfaces (SVIs) in the stack.
  - The ACL to be removed is being used by the policy map.
  - There are three or more switches in the stack.

  The delay can increase, up to 30 minutes, depending on the number of SVIs that are attached to the policy map. The delay does not affect the operation of the policy-map. However, either of these workarounds will reduce the length of the delay:

  - Remove the access control entries (ACEs) from the destination ACL, leaving the ACL empty. (The effect is the same as removing the ACL itself.)
  - Detach the affected policy-maps from all the attached VLANs and SVIs, remove the ACL from the policy-maps, and then *reattach* the policy-maps back to the original SVIs.

- CSCsk19926

  Traffic is not received on a member port in a switch stack under these conditions:

  - The port is in a cross-stack EtherChannel.
  - One or more of the master switch Cisco TwinGig Converter Module ports are in the cross-stack EtherChannel.
  - This member switch has been reloaded.

  The workaround is to enter the **shutdown** and **no shutdown** interface configuration commands on the affected interface or to reload the entire stack instead of a single member switch.

- CSCsl49153

  You might receive a traceback message when you use the **no interface port-channel** global configuration command to delete interfaces from an EtherChannel that has port channels on multiple stack members.

  The workaround is to save the configuration and to reload the stack.

- CSCsl63862

  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.

- CSCso15367

  The CLI output for the StackWise Plus port 2 shows the output for the StackWise Plus port 1 and vice versa.

  There is no workaround.

- CSCso96778

  When you use the **ipv6 address dhcp** interface configuration command on an interface that is configured in router mode, other addresses on the prefix associated with the new address might not be accessible.

  The workaround is to use the **ipv6 address dhcp** interface configuration command on an interface that is configured in host mode, or configure a static route to the prefix through the interface.

- CSCsw68528

  On switches running Cisco IOS Release 12.2(44)SE or 12.2(46)SE, when you enter the **show mvr interface** *interface-id* **members** privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as *ACTIVE*.

  The workaround is to use the **show mvr interface** *interface-id* or the **show mvr members** privileged EXEC command. These command outputs show the correct status of an MVR port.

- CSCsw69015

  When you enter the **mvr vlan** *vlan-id* global configuration command to create an MVR VLAN and enable MVR on the switch by entering the **mvr** global configuration command, if you enter the **show mvr interface** *interface-id* **members** privileged EXEC command, the output shows the MVR groups on the interface. However, if you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly.

- CSCsw96933

  A switch running Cisco IOS Release 12.2(46)SE might lose packets for up to 30 seconds when a link fails. This occurs in some multiple spanning-tree (MST) topologies.

  There is no workaround.

- CSCsz88857

  When an interface on the stack master is a member of an EtherChannel and the channel group number is removed before a master switch changeover, you can not use the same group number when you recreate the EtherChannel after the changeover.

  These are possible workarounds:

  - Reload the switches in the EtherChannel into the channel group that you were not able to create.
  - Use a new channel group number to bundle the physical interfaces in an EtherChannel.
  - Reconfigure the EtherChannel before the master switch changeover.

- CSCta57846

  The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

  The workaround is to enter the **logging file flash**:*filename* global configuration command to configure logging to flash instead of copying to flash.

- CSCtf35960

  When periodic port-based reauthentication is enabled and a new stack master is elected, the stack does not reauthenticate a connected client.

  The workaround is to enter the **dot1x re-authenticate interface** *interface-id* privileged EXEC command to reauthenticate the client.

- CSCti79385

  When a redirect URL is configured for a client on the authentication server and a large number of clients are authenticated, high CPU usage could occur on the switch.

  There is no workaround.

Resolved Caveats

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE5

- 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

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE4

- CSCsh59019

  Authentication, authorization, and accounting (AAA) fails, preventing authentication and requiring you to recover your password. For example, when you enter the **aaa authentication login default group tacacs line** global configuration command, AAA fails.

  There is no workaround.

- CSCsk85192

  When you use an access control server (ACS) to enable command authorization, the ACS does not process a **copy** command ending with a colon (for example, *scp***:**, *ftp***:**, *tftp***:**, *flash***:**).

  This problem affects authentication, authorization, and accounting (AAA) authorization:

  - If the ACS denies a **copy** command ending with a colon, you *can* use that command on a switch.
  - If the ACS permits a **copy** command ending with a colon, you *cannot* use that command on a switch.

  To workaround is to either deny or permit the **copy** command without entering any arguments on the ACS.

- CSCsx97605

  The CISCO-RTTMON-MIB is not correctly implemented in this release.

  There is no workaround.

- CSCsy83366

  On a switch that is configured for quality of service (QoS), a memory leak occurs when a small portion (about 90 bytes) of the processor memory is not released by the HRPC QoS request handler process.

  There is no workaround.

- CSCsy90265

  If you repeatedly enter the **show tech-support** privileged EXEC command, the switch might leak memory and, in some cases, shut down.

  The workaround is to reload the switch to clear the memory after repeated use of the **show tech-support** command.

- CSCsz66428

  When flow control is enabled on a port-channel interface and you enter the flowcontrol receive on interface configuration command, the bundle is not enabled after the switch restarts. The command appears in the port-channel interface running configuration but does not appear in the switch running configuration. A message such as this appears:

  ```
  %EC-5-CANNOT_BUNDLE2: Gi0/27 is not compatible with Po1 and will be suspended (flow
  control receive of Gi0/27 is on, Po1 is off)
  %EC-5-CANNOT_BUNDLE2: Gi0/28 is not compatible with Po1 and will be suspended (flow
  control receive of Gi0/28 is on, Po1 is off)
  ```

Use one of these workarounds:

- To manually configure the port-channel interface, enter the flowcontrol receive on interface configuration command.
- To add the flow-control configuration to the interface after the switch restarts, use an EEM script similar to this:

  ```
  event manager applet Add_flowcontrol_on_restart
  event syslog pattern SYS-5-RESTART
  action 1 cli command "en"
  action 2 cli command "conf t"
  action 3 cli command "inter port 1"
  action 4 cli command "flowcontrol receive on"
  ```

  For *action 3*, specify the port-channel interface.

- CSCsz72234

  In a VPN routing/forwarding (VRF) instance, a port channel is configured, and the default route is in the global routing table. If a link shuts down while the other links remain up, the port channel might not forward traffic.

  Use one of these workarounds:

  - Enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command.
  - In the VRF instance, configure the links in the port channel as Layer 2 access links, and configure a switch virtual interface (SVI).

- CSCta09189

  Packet loss and output drops occur on the egress interface for routed multicast traffic.

  This problem occurs when multiple S,G entries time out at the same time and then are re-established at the same time, when multiple Protocol Independent Multicast (PIM) neighbors time out at the same time and then are re-established at the same time, or when multiple high-volume multicast streams are routed through multiple Layer-3 interfaces.

  Use one of these workarounds:

  - Enter the **clear ip mroute *** EXEC command.
  - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the egress interface.

- CSCta53893

  If the host is in multiple-authentication (multiauth) mode and you configure the fallback authentication process as IEEE 802.1x or MAC authentication bypass, the per-user ACL does not work when the port uses web authentication as the fallback method and then uses 802.1x or MAC authentication bypass as the fallback method.

  The workaround is to restart the switch.

- CSCta57846

  The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

  The workaround is to enter the **logging file** *flash:filename* global configuration command to configure logging to flash instead of copying to flash.

- CSCta78502

  When you have configured a login banner by entering the **banner login** *c message c* global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.

  There is no workaround.

- CSCta87523

  When you use Auto Smartports macros on an interface that is connected to an Cisco IP phone, the the quality of service (QoS) configuration for that interface is not completed.

  The workaround is to enter the **no mls qos vlan-based** interface configuration command, and then enable QoS for voice over IP (VoIP) by entering the **auto qos voip cisco-phone** interface configuration command.

- CSCtb08426

  When two switch stacks are connected, when the stack master fails, and when another switch becomes the stack master, convergence is delayed under these conditions:

  – The stack master has an active EtherChannel in Link Aggregation Control Protocol (LACP) mode.

  – The EtherChannel is cross-stacked.

  – There are two or more switches in each stack.

  The workaround is to not use the EtherChannel LACP mode. Use the EtherChannel on mode to force ports to join an EtherChannel without negotiations.

- CSCtb10158

  A switch can fail when an SNMP process attempts to configure dot1x authentication when it is already configured.

  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.

- CSCtb56844

  After you have entered the **authentication control-direction in** interface configuration command on an authenticator switch port, authentication is successful and the port is in the authorized state. However, another switch that functions as the supplicant cannot pass any traffic over the trunk except for traffic on the native VLAN.

  The workaround is to enter the **no authentication control-direction** interface configuration command on the authenticator port, and then enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to trigger a new authentication.

- CSCtb77378

  When you use IEEE 802.1x authentication with web authentication and an HTTP page opens, the switch redirects the user to an HTTP login page, not a HTTPS login page.

  The workaround is to remove the custom banner.

- CSCtb84303

  In a switch stack, when the SNMP vlan change (vmMembershipEntry) MIB is sent to a member switch other than the stack master, line protocol and notification flapping occurs.

  There is no workaround.

- CSCtb91572

  A switch enters a loop in which it continues to fail after it first has failed while starting, and then has failed again while attempting to recover. This failure loop occurs only after you have entered the **archive upload-sw** privileged EXEC command to write the configuration to a remote server using Secure Copy Protocol (SCP) and when the connection to the remote server is configured for spanning-tree PortFast.

  The workaround is to not use SCP to write to the remote server. Use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

- CSCtc39809

  A memory leak occurs when there is a stuck in active (SIA) state condition for an Enhanced Interior Gateway Routing Protocol (EIGRP) route.

  There is no workaround.

- CSCtc43231

  A switch does not receive SNMP trap and inform messages from the correct interface after you have entered the **snmp-server trap-source loopback0** and **snmp-server source-interface informs loopback0** global configuration commands.

  There is no workaround.

- CSCtc57809

  When the **no mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command is used to remove a dynamically learned MAC address, the switch fails under these conditions:

  - The physical interface is in a *no shut* state.
  - The MAC address is first dynamically learned and then changed to static.

  There is no workaround.

- CSCtc70571

  When you have configured an output service policy, performing an SNMPWALK on cportQosStatistics causes loops.

  There is no workaround.

- CSCtc71798

  Traffic received on a member interface of a cross-stack EtherChannel is dropped from a switch stack. This intermittently occurred in previous releases after a stack reloaded.

  There is no workaround.

- CSCtc81879

  After all member ports are brought up on a switch stack, MAC authentication bypass (MAB) authenticates the stack master ports but not any member switch ports. The symptom occurs after you have entered both the **switchport port-security** interface configuration command and the **dot1x control-direction** interface configuration command on the stack interfaces.

  The workaround is to enter either the **no switchport port-security** interface configuration command or the **no dot1x control-direction** interface configuration command on the stack interfaces.

- CSCtc90039

  A memory leak occurs on a device that uses Enhanced Interior Gateway Routing Protocol (EIGRP) when the external routes are being exchanged.

  The workaround is to stabilize the network to minimize the impact of external route advertisement.

- CSCtd17296

  When you enter the **dot1x pae** interface configuration command on a switch access port and then enable an access list in the inbound direction on an ingress switched virtual interface (SVI), the access list does not work, allowing all packets to pass.

  The workaround is to enable the access list in the outbound direction on the egress SVI.

- CSCtd30053

  When you enter the **no spanning-tree etherchannel guard misconfig** global configuration command, enter the **write memory** privileged EXEC command, and then restart the switch, the **spanning-tree etherchannel guard misconfig** global configuration command is saved instead of the **no** form of this command.

  There is no workaround.

- CSCtd31242

  An IP phone loses network connectivity under these conditions:

  - The IP phone is authenticated by MAB (in Open1x mode) on a supplicant switch.
  - The supplicant switch is connected to an authenticator switch through the NEAT protocol.

  A call is placed using the IP phone. After approximately 5 minutes, network connectivity to the phone is lost.

  The workaround is to statically configure the MAC address of the IP phone on the authenticator switch.

- CSCtd72456

  After you have entered the **snmp-server host informs** global configuration command to enable SNMP informs on a switch, the switch might fail if you enter the **show snmp pending** user EXEC command.

  There is no workaround. Do not enter the show command when SNMP informs are enabled.

- CSCtd72626

  A Remote Switched Port Analyzer (RSPAN) does not detect IPv6 multicast packets on an RSPAN destination port.

  There is no workaround.

- CSCtd73256

  A switch fails when you enter the **show ip ospf interface** user EXEC command and then stop the command output at the this line:

  ```
  Backup Designated router (ID) xx.x.x.x, Interface address xx.x.x.x
  ```

  The failure occurs when the Backup Designated Router (BDR) neighbor of the switch is shut down while you press Enter or the spacebar to advance the command output.

  When the switch fails, it sends this error message:

  ```
  Unexpected exception to CPUvector 2000, PC = 261FC60
  ```

  There is no workaround.

- CSCte00827

  On a switch that has one port configured as a Switched Port Analyzer (SPAN) source port, a memory leak occurs when a Power-over-Ethernet (PoE) port link goes up and down.

  There is no workaround.

- CSCte67201

  On a switch that is configured for IP routing and that is running Cisco IOS Release 12.2(50)SE or later, Cisco Express Forwarding (CEF) can use a large amount of memory. The IP RIB Update process uses about 2000 bytes for each prefix that CEF uses.

  There is no workaround. You can reduce the memory use by reducing the number of routes the switch processes.

- CSCte81321

  After you have entered the **logging filter** global configuration command on a switch to specify a syslog filter module to be used by the Embedded Syslog Manager (ESM), processes logging many system messages retain increasing amounts of processor memory.

  The workaround is to enter the **no logging filter** global configuration command.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE3

- CSCsl72774

  Memory allocation errors no longer occur when the Cisco Express Forwarding (CEF) consistency checkers have been enabled. The CEF consistency checkers have been enabled by default. They can also be enabled by using these global configuration commands:

  cef table consistency-check ipv4

  cef table consistency-check ipv6

- CSCso57496

  A switch no longer fails when you enter the **configure replace** privileged EXEC command, and a banner is already present in the switch configuration.

- CSCso90107

  You can now query the bgpPeerTable MIB for VPN/VRF interfaces.

- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

- CSCsq51052

  The output of the **show ip ssh** privileged EXEC command no longer displays *SSH Enabled - version 2.99*. Instead, a correct SSH version (*1.5*, *1.99* or *2.0*) now appears.

- CSCsy15227

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

- CSCsy07555

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCsx70889

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCta32597

  A switch no longer fails when a host moves from a dynamically assigned VLAN to a configured VLAN.

- CSCta36155

  A switch configured with 802.1x and port security on the same ports no longer might inappropriately put the ports into an error-disabled state.

- CSCta56469

  Moving a PC between two IP Phones without disconnecting either phone from the switch no longer triggers a port-security violation.

- CSCta67777

  A port security violation error no longer occurs when MAC address sticky learning is enabled on a port and a CDP is enabled on a connected IP Phone.

- CSCsv32556

  A Telnet, Secure Shell (SSH), or console session on the switch no longer fails when you use the **show file systems** EXEC command or when you access the remote file system, flash*n*: (where *n* is the switch number).

- CSCsw45277

  Third-party IP phones now automatically power up when reconnected to enabled PoE ports on the switch.

- CSCsx36608

  If a large number of clients in a switch stack use MAC authentication bypass to authenticate at the same time, the clients are no longer in the unauthorized state when

  - The stack members start at the same time because the stack reloaded or powered up.
  - The RADIUS server is down, the re-authentication timer expires, all the ports become unauthorized, and the RADIUS restarts.
  - All the ports on stack members are disabled and then re-enabled with the shutdown and no shutdown interface configuration commands at the same time.
  - The wake-on-LAN (WoL) feature is enabled and a large number of clients try to authenticate.

- CSCsx49718

  Re-authentication now occurs on a port under these conditions:

  - The port is in single-host mode.
  - The port is configured with the **authentication event no-response action authorize vlan** *vlan-number* command.
  - An EAPOL start packet is sent to the port.

- CSCsx94339

  A switch no longer fails and reloads when a specific queue is removed from a class:

  ```
  class-map match-any CMAP-BC-ALL-COS
   match cos  2
   match cos  1

  policy-map PMAP-ingress-g0/1
    class CMAP-BC-ALL-COS
      no queue-limit cos  1 200
  ```

- CSCsy27389

  The switch now changes the time in an EnergyWise recurrence event when the local time changes to daylight saving time.

- CSCsy34739

  A trunk port no longer goes into the error-disabled state when the trunk port’s native VLAN is in a suspended state or is not configured on the switch itself.

- CSCsy48370

  The switch no longer fails when you use the **vacant-message** line configuration command.

- CSCsy57970

  When IEEE 802.1x multiple authentication mode is configured on a port, two PCs have been authenticated, and the first PC is disconnected, the second PC now receives and forwards traffic on the port.

- CSCsy72669

  If a link failure occurs on a secondary edge port, preemption now occurs after the link comes up.

- CSCsz05975

  A stack member no longer fails when the hostname is longer than 36 characters.

- CSCsz12381

  When open1x authentication and MAC authentication bypass are enabled on a port, an IP phone is connected to the port, and DHCP snooping is enabled on the switch, DHCP traffic is now forwarded on the voice VLAN before open 1x authentication times out and the switch uses MAC authentication bypass to authorize the port.

- CSCsz13490

  The switch no longer reloads when you enter several key strokes while in interface-range configuration mode.

- CSCsz14369

  If MAC authentication bypass is enabled and the RADIUS server is not available, the switch now tries to re-authenticate a port after a server becomes available.

- CSCsz68923

  A TwinGig Converter module in slot 2 is now correctly recognized by the switch software.

- CSCsz77920

  If you are configuring Flexible Authentication Ordering with web authentication on a switch port and the switch uses 802.1x to authenticate the host, Address Resolution Protocol (ARP) now works properly.

- CSCsz79293

  When VPN routing and forwarding (VRF) is configured on the stack master, communication no longer fails after the stack master has shut down.

- CSCsz81762

  If you enable automatic server testing through the **radius-server host** *ip-address* [**test username** *name*] global configuration command, the switch no longer sends requests to the RADIUS server if the server is not available.

- CSCsz89393

  SNMP queries to the Bridge-MIB now operate on switch stacks with five or more stack members and a large number of active ports.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE1

- CSCsb46724

  If the connection to a primary AAA server fails, the backup server is now queried for login access.

- CSCsr92741

  When a TCP packet with all flags set to zero (at the TCP level) is sent to a remote router, the remote (destination) router no longer returns an ACK/RST packet back to the source of the TCP segment.

- CSCsy24510

  The switch now accepts an encrypted secret password.

- CSCsy41470

  The switch no longer runs out of memory when an smnpwalk, snmpget, or snmpbulkwalk is run on the CISCO-ENERGYWISE-MIB.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE

- 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.

- 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

- CSCso53157

  When STP is disabled on the stack, the Hot Standby Router Protocol (HSRP) hello packets now pass through the switch stack when the stack is connected to two routers through cross-stack EtherChannels.

- CSCsq2687

  The server no longer attempts re-authentication every ten minutes when a switch is configured with the **dot1x timeout reauth-period server** interface configuration command.

- CSCsq67398

  Traffic is now forwarded to the interfaces that are configured with static multicast MAC addresses after the switch is reloaded.

Note You cannot configure the static MAC address (unicast or multicast) entries on EtherChannel member interfaces, or add an interface into the EtherChannel if that interface is associated with a static MAC address entry.

- CSCsq89564

  If the switch uses 802.1x authentication with VLAN assignment, it no longer uses the VLAN assignment with different authorization attempts, such as user authentication or re-authentication.

- 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

- CSCsr50766

  When keepalive is disabled on an interface, the interface is no longer put in an error-disabled state when it receives keepalive packets.

- CSCsr64007

  The Switched Port Analyzer (SPAN) destination port no longer detects IPv6 multicast packets from a VLAN that is not being monitored by SPAN.

- CSCsr65689

  This message no longer appears in the log during the system bootup on a switch that is running Cisco IOS 12.2(50)SE:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2
  ```

- CSCsu10065

  When SFP ports are configured as status multicast router ports, IPv6 Multicast Listener Discovery (MLD) snooping now works after the switch reloads.

- CSCsu59214

  The `Set TxPortFifo SRR Failed` message no longer appears when you enter both the s**rr-queue bandwidth shape 200 0 2 200** and the **priority-queue out** interface configuration commands on the same interface.

- CSCsu88168

  The switch no longer reloads when the Forwarding Information Base (FIB) adjacency table is added.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website 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-20090908-tcp24.shtml.

- CSCsv30429

  A Cisco IP Phone connected to a Catalyst switch no longer becomes unauthorized when it transitions from the data authorization domain to the voice authorization domain.

- 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.

- CSCsv64023

  A switch port configured for IGMP snooping no longer lose its group membership when the port receives a query comes from an upstream device that is not configured for IGMP snooping.

- CSCsv89005

  A switch configured with class-based policies that are applied and active on at least one interface no longer might reload or display CPU hog messages during SNMP polling for the ciscoCBQosMIB.

- CSCsv91358

  When you have entered the **vlan dot1q tag native** global configuration command to configure a switch to tag native VLAN frames on 802.1Q trunk ports, and you configure a new voice VLAN on an access port, the MAC address of a connected PC is now correctly relearned.

- CSCsw30249

  When a switch virtual interface (SVI) is configured as unnumbered and is pointing to a loopback interface, the switch no longer fails when the SVI receives a packet.

- CSCsw45337

  When LLDP is enabled and a voice VLAN is configured, the L2 Priority and DSCP Value fields in the LLDP type, length, and value descriptions (TLVs) are now correctly marked to give the voice traffic the correct DSCP and Layer 2 priority.

- CSCsw65548

  Switch ports no longer attempt authentication at the interval configured for the port security timer instead of the configured IEEE 802.1x timer.

Documentation Updates

- Update to the Software Documentation, page 36
- Updates to the Command Reference, page 36
- Updates to the Switch Getting Started Guide, page 38
- Updates for the System Message Guide, page 38

Update to the Software Documentation

The switch does not support ISL trunking.

The switch does not support Cisco EnergyWise.

Updates to the Command Reference

debug authentication

Use the **debug authentication** privileged EXEC command to enable debugging of the authentication settings on an interface. Use the **no** form of this command to disable debugging.

debug authentication {**all** | **errors** | **events** | **sync** | **feature** [**all**] [**acct**] [**auth_fail_vlan**] [**auth_policy**] [**autocfg**] [**critical**] [**dhcp**] [**guest_vlan**] [**mab_pm**] [**mda**] [**multi_auth**] [**switch_pm**] [**switch_sync**] [**vlan_assign**] [**voice**] [**webauth**] [**all** | **errors** | **events**]}

no debug authentication {**all** | **errors** | **events** | **sync** | **feature** [**all**] [**acct**] [**auth_fail_vlan**] [**auth_policy**] [**autocfg**] [**critical**] [**dhcp**] [**guest_vlan**] [**mab_pm**] [**mda**] [**multi_auth**] [**switch_pm**] [**switch_sync**] [**vlan_assign**] [**voice**] [**webauth**] [**all** | **errors** | **events**]}

Syntax Description

acct	(Optional) Display authentication manager accounting information.
all	(Optional) Display all authentication manager debug messages.
auth_fail_vlan	(Optional) Display authentication manager errors for the restricted VLAN.
auth_policy	(Optional) Display authentication policy messages.
autocfg	(Optional) Display autoconfiguration authentication manager debug messages.
critical	(Optional) Display the inaccessible authentication bypass messages. **Note** The inaccessible authentication bypass feature is also referred to as critical authentication or the authentication, authorization, and accounting (AAA) fail policy.
dhcp	(Optional) Display authentication manager debug messages on DHCP dynamic address-enable interfaces.
errors	(Optional) Display all authentication manager error debug messages.
events	(Optional) Display all authentication manager event debug messages, including registry and miscellaneous events.
feature	(Optional) Display authentication manager feature debug messages
guest_vlan	(Optional) Display guest VLAN authentication manager messages.
mab_pm	(Optional) Display MAC authentication manager bypass authentication debug messages.
mda	(Optional) Display multidomain authentication manager debug messages.
multi_auth	(Optional) Display multi-authentication manager debug authentication messages.
switch_pm	(Optional) Display switch port manager messages.

switch_sync	(Optional) Display synchronization messages between the switch, the authentication server, and the connected devices.
sync	(Optional) Display operational synchronization authentication manager debug messages.
vlan_assign	(Optional) Display the VLAN-assignment debug messages.
voice	(Optional) Display the voice-VLAN debug messages.
webauth	(Optional) Display web authentication manager debug messages.

Defaults

Authentication debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(50)SE	This command was introduced.

Usage Guidelines

The **undebug authentication** command is the same as the **no debug authentication** command.

On stacking switches, when you enable debugging, it is enabled only on the stack master.

To enable debugging on a stack member, you can start a session from the stack master by using the **session switch-number** privileged EXEC command and then entering the **debug authentication** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number** *line* privileged EXEC command on the stack master switch to enable debugging on a stack member.

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.

Command	Description
authentication priority	Adds an authentication method to the port-priority list.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
show authentication	Displays information about authentication manager events on the switch.

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

These messages were added:

Error Message `ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]`

Explanation There are insufficient resources available to create a hardware representation of the ACL. A lack of available logical operation units or specialized hardware resources can cause this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Recommended Action Modify the ACL configuration to use fewer resources, or rename the ACL with a name or number that alphanumerically precedes the other ACL names or numbers.

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

Explanation Authentication was unsuccessful. The first [chars] is the hostname, and the second [chars] is the interface.

Recommended Action No action is required.

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

Explanation Authentication was successful. The first [chars] is the host name, and the second [chars] is the interface.

Recommended Action No action is required.

Error Message `%DOT1X_SWITCH-4-PROC_START_ERR: Unable to start dot1x switch process.`

Explanation The software could not start the 802.1x authentication process.

Recommended Action Use the **reload** privileged EXEC command to reload the switch.

Error Message `%EC-5-MINLINKS_MET: Port-channel [chars] is up as its bundled ports ([dec]) meets min-links`

Recommended Action The administrative configuration of minimum links is equal to or less than the number of EtherChannel ports. The port channel is up. [chars] is the EtherChannel, and [dec] is the EtherChannel group number.

Recommended Action No action is required.

Error Message `%EC-5-MINLINKS_NOTMET: Port-channel [chars] is down bundled ports ([dec]) doesn't meet min-links`

Explanation The administrative configuration of minimum links is greater than the number of bundled ports. The port channel is down. [chars] is the EtherChannel, and [dec] is the EtherChannel group number.

Recommended Action Reduce the value of the minimum-links configuration parameter for an EtherChannel, or add more ports to the EtherChannel to create a bundle.

Error Message `%IP_DEVICE_TRACKING_HA-3-FAIL_SEND_MSG_TO_ACTIVE: Failed to send [chars] message to active for [chars], [chars]`

Explanation The Inter-Process Communication (IPC) synchronization message was could not sent to the stack member in the run-time module because of a software error. For more information, see the message on the console or in the system log. The system state between the stack members and provisioned switches might not be synchronized. The first [chars] is the synchronization message, the second [chars] is the stack master number, and the third [chars] is the run-time module.

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. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. 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. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section on page 2-7.

Error Message `%IP_DEVICE_TRACKING_HA-3-NO_RESOURCES: [chars]`

Recommended Action The software could not get the required resources to complete a task. This was probably caused by a software error or a lack of available memory. For more information, see the message on the console or in the system log. The system state between the active and standby units might not be synchronized. [chars] is message.

Recommended Action If a lack of available memory caused the problem, reduce other system activity, or allocate more memory for this task. If the problem recurs, 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. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. 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. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section on page 2-7.

Error Message `%PAGP_DUAL_ACTIVE-3-OBJECT_CREATE_FAILED: Unable to create [chars]`

Explanation The switch cannot create the specified managed object. [chars] is the object name.

Recommended Action No action is required.

Error Message `%PAGP_DUAL_ACTIVE-3-RECOVERY_TRIGGER: PAgP running on [chars] informing virtual switches of dual-active: new active id [enet], old id [enet]`

Explanation Port Aggregation Protocol (PAgP) received a new active ID on the specified interface, which means that all virtual switches are in a dual-active scenario. The interface is informing virtual switches of this, which causes one switch to go into recovery mode. [chars] is the interface. The first [enet] is the new active ID. The second [enet] is the ID that it replaces.

Recommended Action No action is required.

Error Message `%PAGP_DUAL_ACTIVE-3-REGISTRY_ADD_ERR: Failure in adding to [chars] registry`

Explanation The switch could not add a function to the registry. [chars] is the registry name.

Recommended Action No action is required.

Error Message `%PHY-4-SFP_PLUS_NOT_SUPPORTED: The SFP PLUS in [chars] is not supported`

Explanation The Cisco X2 transceiver module is not supported on the switch. [chars] is the port in which the SFP module is inserted.

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. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error. 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. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section on page 2-7.

Error Message `%PM-6-EXT_VLAN_ADDITION: Extended VLAN is not allowed to be configured in VTP CLIENT mode.`

Explanation The switch did not add a VLAN in VTP client mode.

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. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the system message guides.

Error Message `%SPANTREE_VLAN_SHIM-3-ADD_REGISTRY_FAILED: Subsystem [chars] fails to add callback function [chars]`

Explanation A subsystem has added its callback functions. Use this message only for debugging. The first [chars] is the subsystem name, and the second [chars] is the function name.

Recommended Action No action is required.

Error Message `%SPANTREE_VLAN_SHIM-2-MAX_INSTANCE: Platform limit of [dec] STP instances exceeded. No instance created for [chars] (port [chars]).`

Explanation The number of VLAN spanning-tree instances has reached the allowable maximum. No more VLAN instances are created until instances are less than the maximum. [dec] is the maximum, the first [chars] is the VLAN for which an STP instance is not created, and the second [chars] is the port number.

For example, when you are configuring spanning tree and the allowable maximum is 128 instances

- If the switch has already created 128 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 200, and an STP instance for VLAN 200 is not created.
- If the switch has already created 100 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 228. The switch creates STP instances for VLAN 200 to VLAN 227, but not for VLAN 228. 200 is not created.

STP instances are also not created for the remainder of the VLANs in the range

Recommended Action Reduce the number of active spanning-tree instances by either disabling some or deleting the VLANs associated with them. To create STP instances, manually create them. If you do not, the switch automatically creates an STP instances when a VLAN is created.

For example, if the switch has already created 128 instances and you want to create an STP instance for VLAN 200, remove a spanning-tree instance with one of these commands:

- To delete one of the VLANs with an STP instance, enter the **no vlan** *vlan-id* global configuration command.
- To disable spanning tree on a per-VLAN basis. enter the **no spanning-tree** *vlan-id* global configuration command.

Then enter the **spanning-tree 200** global configuration command to create an instance for VLAN 200.

These messages have been deleted:

Error Message `ACLMGR-2-NOVMR: Cannot create VMR data structures for access list [chars].`

Error Message `DOT1X-5-INVALID_INPUT: Dot1x Interface parameter is Invalid on interface [chars].`

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

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

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

Error Message `UDLD-3-UDLD_IDB_ERROR: UDLD error handling [chars] interface [chars].`

Error Message `UDLD-3-UDLD_INTERNAL_ERROR: UDLD internal error [chars].`

Error Message `UDLD-3-UDLD_INTERNAL_IF_ERROR: UDLD internal error, interface [chars] [chars].`

Error Message `UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface [chars], [chars] detected.`

Error Message `UDLD-6-UDLD_PORT_RESET: UDLD reset interface [chars].`

Error Message `UFAST_MCAST_SW-3-PROC_START_ERROR: No process available for transmitting UplinkFast packets.`

Error Message UFAST_MCAST_SW-4-MEM_NOT_AVAILABLE: No memory is available for transmitting UplinkFast packets on Vlan [dec].

Error Message VQPCLIENT-2-CHUNKFAIL: Could not allocate memory for VQP.

Error Message VQPCLIENT-2-DENY: Host [enet] denied on interface [chars].

Error Message %VQPCLIENT-2-INITFAIL: Platform-specific VQP initialization failed. Quitting

Error Message %VQPCLIENT-2-IPSOCK: Could not obtain IP socket

Error Message %VQPCLIENT-7-NEXTSERV: Trying next VMPS [IP_address]

Error Message %VQPCLIENT-7-PROBE: Probing primary server [IP_address]

Error Message %VQPCLIENT-2-PROCFAIL: Could not create process for VQP. Quitting

Error Message %VQPCLIENT-7-RECONF: Reconfirming VMPS responses

Error Message %VQPCLIENT-2-SHUTDOWN: Interface [chars] shutdown by VMPS

Error Message %VQPCLIENT-3-THROTTLE: Throttling VLAN change on [chars]

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*

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*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

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

  SFP 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

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.