Release Notes for the Catalyst 3750, 3560, 2960-S, and 2960 Switches, Cisco IOS Release 12.2(58)SE1 and Later

Revised December 22, 2011

Note Cisco IOS Release 12.2(58)SE images for all platforms were removed from Cisco.com because of a severe defect, CSCto62631. The solution for the defect is in Cisco IOS Release 12.2(58)SE1.

Cisco IOS Release 12.2(58)SE1 runs on Catalyst 3750, 3560, 2960-S, and 2960 switches and on Cisco EtherSwitch service modules. Not all Catalyst 3750 and 3560 switches can run this release. The models listed below are *not* supported in Cisco IOS Release 12.2(58)SE1 and later. For ongoing maintenance rebuilds for these models, use Cisco IOS Release 12.2(55)SE and later (SE1, SE2, and so on).

- WS-C3560-24TS
- WS-C3560-24PS
- WS-C3560-48PS
- WS-C3560-48TS
- WS-C3750-24PS
- WS-C3750-24TS
- WS-C3750-48PS
- WS-C3750-48TS
- WS-3750G-24T
- WS-C3750G-12
- WS-C3750G-24TS
- WS-C3750G-16TD

The Catalyst 3750 switches and the Cisco EtherSwitch service modules support stacking through Cisco StackWise technology. The Catalyst 3560 and 2960 switches do not support switch stacking. Catalyst 2960-S does support stacking. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

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

These release notes include important information about Cisco IOS Release 12.2(58)SE1 and any limitations, restrictions, and caveats that apply to the releases. 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 8.
- 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 8.

You can download the switch software from this site (registered Cisco.com users with a login password):
http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.html=rpm

Contents

System Requirements

Supported Hardware

Table 1 Catalyst 3750 and Cisco EtherSwitch Service Modules Supported

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750G-24WS-S25	24 10/100/1000 PoE[1] ports, 2 SFP[2] module slots, and an integrated wireless LAN controller supporting up to 25 access points.	Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE
Catalyst 3750G-24WS-S50	24 10/100/1000 PoE ports, 2 SFP module slots, and an integrated wireless LAN controller supporting up to 50 access points	Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE
Catalyst 3750-24FS	24 100BASE-FX ports and 2 SFP module slots	Cisco IOS Release 12.2(25)SEB
Catalyst 3750G-24PS	24 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-24TS-1U	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750V2-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-48PS	48 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-48TS	48 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-24FS	24 SFP module slots and 2 SFP module slots	Cisco IOS Release 12.2(55)EY
NME-16ES-1G[3]	16 10/100 ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide	Cisco IOS Release 12.2(25)SEC
NME-16ES-1G-P[4]	16 10/100 PoE ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide	Cisco IOS Release 12.2(25)EZ
NME-X-23ES-1G[4]	23 10/100 ports, 1 10/100/1000 PoE port, no StackWise connector ports, extended single-wide	Cisco IOS Release 12.2(25)SEC
NME-X-23ES-1G-P[4]	23 10/100 PoE ports, 1 10/100/1000 PoE port, no StackWise connector ports, extended single-wide	Cisco IOS Release 12.2(25)EZ
NME-XD-24ES-1S-P[4]	24 10/100 PoE ports, 1 SFP module port, 2 StackWise connector ports, extended double-wide	Cisco IOS Release 12.2(25)EZ
NME-XD-48ES-2S-P[4]	48 10/100 PoE ports, 2 SFP module ports, no StackWise connector ports, extended double-wide	Cisco IOS Release 12.2(25)EZ

1. PoE = Power over Ethernet
2. SFP = small form-factor pluggable
3. Cisco EtherSwitch service module

Table 2 Catalyst 3560 Switches Supported

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3560-8PC	8 10/100 PoE ports and 1 dual-purpose port[1] (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 3560G-24PS	24 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-12PC Compact Switch	12 Ethernet 10/100 ports with PoE and 1 dual-purpose 10/100/1000 or SFP uplink	Cisco IOS Release 12.2(50)SE
Catalyst 3560V2-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-48PS	48 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-48TS	48 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-24TS-SD	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1

1. Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.

Table 3 Catalyst 2960, and 2960-S Switches Supported

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960-48PST-S	48 10/100 PoE ports, 2 10/100/1000 ports, and 2 SFP module slots	Cisco IOS Release 12.2(50)SE2
Catalyst 2960-24PC-S	24 10/100 PoE ports and 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP module slots)	Cisco IOS Release 12.2(50)SE2
Catalyst 2960-24LC-S	24 10/100 ports (8 of which are PoE) and 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP module slots)	Cisco IOS Release 12.2(50)SE2
Catalyst 2960-8TC-S	8 10/100 ports and 1 dual-purpose port[3] (1 10/100/1000BASE-T copper port and1 SFP module slot)	Cisco IOS Release 12.2(46)SE
Catalyst 2960-48TT-S	48 10/100 ports and 1 10/100/1000 ports	Cisco IOS Release 12.2(46)SE
Catalyst 2960-48PST-L	48 10/100 PoE ports, 1 10/100/1000 ports and 2 SFP module slots	Cisco IOS Release 12.2(46)SE
Catalyst 2960-24-S	24 10/100 BASE-TX Ethernet ports	Cisco IOS Release 12.2(37)EY

Table 3 Catalyst 2960, and 2960-S Switches Supported (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960-24TC-S	24 10/100BASE-T Ethernet ports and 2 dual-purpose ports (two 10/100/1000BASE-T copper ports and two SFP module slots)	Cisco IOS Release 12.2(37)EY
Catalyst 2960-48TC-S	48 10/100BASE-T Ethernet ports and 2 dual-purpose ports (two 10/100/1000BASE-T copper ports and two SFP module slots)	Cisco IOS Release 12.2(37)EY
Catalyst 2960PD-8TT-L	8 10/100 ports and 1 10/100/1000 port that receives power	Cisco IOS Release 12.2(44)SE
Catalyst 2960-8TC-L	8 10/100 Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 2960G-8TC-L	7 10/100/1000 Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 2960-24LT-L	24 10/100 ports, 8 of which are PoE, and 2 10/100/1000 ports	Cisco IOS Release 12.2(44)SE
Catalyst 2960-48TC-L	48 10/100BASE-TX Ethernet ports and 2 dual-purpose ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24TC-L	24 10/100BASE-TX Ethernet ports and 2 dual-purpose ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24PC-L	24 10/100 Power over Ethernet (PoE) ports and 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 small form-factor pluggable [SFP] module slots)	Cisco IOS Release 12.2(44)SE
Catalyst 2960-24TT-L	24 10/100BASE-T Ethernet ports and 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-48TT-L	48 10/100BASE-T Ethernet ports 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-24TC-L	24 10/100/1000BASE-T Ethernet ports, including 4 dual-purpose ports (four 10/100/1000BASE-T copper ports and four SFP module slots)	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-48TC-L	48 10/100/1000BASE-T Ethernet ports, including 4 dual-purpose ports (four 10/100/1000BASE-T copper ports and four SFP module slots)	Cisco IOS Release 12.2(25)SEE
Catalyst 2960S-48FPD-L[1]	48 10/100/1000 Power over Ethernet Plus (PoE+) ports (PoE budget of 740 W) and 2 SFP+[2] module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPD-L[1]	48 10/100/1000 PoE+ ports (PoE budget of 370 W) and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PD-L[1]	24 10/100/1000 PoE+ ports (PoE budget of 370 W) and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TD-L[1]	48 10/100/1000 ports and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1

Table 3 Catalyst 2960, and 2960-S Switches Supported (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960S-24TD-L[1]	24 10/100/1000 ports and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48FPS-L[1]	48 10/100/1000 PoE+ ports (PoE budget of 740 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPS-L[1]	48 10/100/1000 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PS-L[1]	24 10/100/1000 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TS-L[1]	48 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TS-L[1]	24 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1

1.Support Cisco FlexStack technology.

2.SFP+ = 10 Gigabit fiber uplink.

Table 4 Other Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
SFP modules (Catalyst 3750 and 3560)	1000BASE-CWDM[1], -LX, SX, -T, -ZX	Cisco IOS Release 12.2(18)SE
	100BASE-FX MMF[2]	Cisco IOS Release 12.2(20)SE
	Support for eight additional DWDM SFP optical modules. For a complete list of supported SFPs and part numbers, see the data sheet: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.html	
SFP modules (Catalyst 2960)	1000BASE-BX, -CWDM, -LX/LH, -SX, -ZX	Cisco IOS Release 12.2(25)FX
	100BASE-BX, FX, -LX	
XENPAK modules[3]	XENPAK-10-GB-ER, XENPAK-10-GB-LR, and XENPAK-10-GB-SR	Cisco IOS Release 12.2(18)SE
Redundant power systems	Cisco RPS 675 Redundant Power System	Supported on all software releases
	Cisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch)	Supported on all software releases
	Cisco Redundant Power System 2300	Cisco IOS Release 12.2(35)SE and later

1. CWDM = coarse wavelength-division multiplexer
2. MMF = multimode fiber
3. XENPAK modules are only supported on the Catalyst 3750G-16TD switches.

Device Manager System Requirements

Hardware Requirements

Table 5 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

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 6.0 or 7.0, and Firefox up to version 27, with JavaScript enabled.

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

Cluster Compatibility

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

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

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, the command reference, and the Cisco EtherSwitch service module feature guide.

CNA Compatibility

Cisco IOS 12.2(50)SE and later is only compatible with Cisco Network Assistant (CNA) 5.0 and later. You can download Cisco Network Assistant from this URL: http://www.cisco.com/cisco/software/navigator.html?mdfid=279230132http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistanti=rp

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

Upgrading the Switch Software

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 For Catalyst 3750 and 3560 switches and the Cisco EtherSwitch service modules, 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 image or IP services image) and does not change if you upgrade the software image.

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 6 Cisco IOS Software Image Files

Filename	Description
c3750-ipbasek9-tar.122-58.SE1.tar	Catalyst 3750 IP base cryptographic image and device manager files. This image has the Kerberos, SSH[1], Layer 2+, and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipservicesk9-tar.122-58.SE1.tar	Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules.
c3560-ipbasek9-tar.122-58.SE1.tar	Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.

Table 6 Cisco IOS Software Image Files (continued)

Filename	Description
c3560-ipservicesk9-tar.122-58.SE1.tar	Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c2960-lanbasek9-tar.122-58.SE1.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanlitek9-tar.122-58.SE1.tar	Catalyst 2960 LAN lite cryptographic image file and device manager files.
c2960s-universalk9-tar.122-58.SE1.tar	LAN Base and LAN Lite crypto image with device manager

1. SSH = Secure Shell.

Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility

The Catalyst 3750 Integrated Wireless LAN Controller Switch is an integrated Catalyst 3750 switch and Cisco 4400 series wireless LAN controller that supports up to 25 or 50 lightweight access points. The switch and the internal controller run separate software versions, which must be upgraded separately.

To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running one of these Cisco IOS software releases:

- Cisco IOS Release 12.2(25)FZ
- Cisco IOS Release 12.2(35)SE or later
- Cisco IOS Release 12.2(37)SE or later
- Cisco IOS Release 12.2(44)SE or later
- Cisco IOS Release 12.2(46)SE or later

Note These Cisco IOS Releases and any versions of them are not supported: Cisco IOS Release 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 images (IP Base, IP Services, and Advanced IP Services) are supported for use with the controller.

If the switch image version is not compatible, the wireless LAN controller switch could stop functioning.

For information about the controller software, see the release notes on this page for Cisco Software Release 4.0.x.0 or later:
http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

For controller software upgrade procedure, see the *Cisco Wireless LAN Controller Configuration Guide* on this page:
.http://www.cisco.com/en/US/products/ps6366/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 to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

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

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

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.

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

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

Step 1 Use Table 6 on page 8 to identify the file that you want to download.

Step 2 Download the software image file:

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

http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

b. Navigate to **Switches > LAN Switches - Access**.

c. Navigate to your switch model.

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

Download the image you identified in Step 1.

Caution If you are upgrading a Catalyst 3750 switch that is running a release earlier than Cisco IOS Release 12.1(19)EA1c, this release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.

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.

The **/allow-feature-upgrade** option allows installation of an image with a different feature set (for example, upgrade from the IP base image to the IP services image).

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/c3750-ipservices-tar.122-50.SE.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 recovery procedures, see the "Troubleshooting" chapter in the software configuration guide for this release.

Installation Notes

Use these methods to assign IP information to your switch:

- 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.

Note If you are upgrading a Catalyst 3750 or a 2950 switch running Cisco IOS Release 12.1(11)AX, which uses the IEEE 802.1x feature, you must re-enable IEEE 802.1x after upgrading the software. For more information, see the "Cisco IOS Notes" section on page 38.

Note When upgrading or downgrading from Cisco IOS Release 12.2(18)SE, you might need to reconfigure the switch with the same password that you were using when running Cisco IOS Release 12.2(18)SE. This problem only occurs when changing from Cisco IOS Release 12.2(18)SE to any other release. (CSCed88768)

New Software Features

- Support for the Built-in Traffic Simulator using Cisco IOS IP SLAs video operations to generate synthetic traffic for a variety of video applications, such as Telepresence, IPTV, and IP video surveillance cameras. You can use the simulator tool:
  - for network assessment before deploying applications with stringent network performance requirements.
  - with Cisco Mediatrace for post-deployment troubleshooting of network-related performance issues.

  The traffic simulator includes a sophisticated scheduler that allows you to run several tests simultaneously or periodically, and over extended time periods. (Catalyst 3750 and 3560)
- Cisco Mediatrace to troubleshoot and isolate network or application issues in traffic streams. It helps drill down to analyze one-way delay, one-way packet loss, one-way jitter, and connectivity in IPv4 networks that carry video traffic. You can use Mediatrace for any UDP-based video or non-video traffic stream. (Catalyst 3750 and 3560)
- Cisco Application Performance Monitor to track the video packet flow and to troubleshoot and isolate performance degradation in traffic streams. You can use the performance monitor for both video and non-video traffic. (Catalyst 3750 and 3560)
- EnergyWise Phase 2.5 enhancements that add support for a query to analyze and display domain information and for Wake on LAN (WoL) to remotely power on a WoL-capable PC.
- Smart logging to capture and export packet flows to a NetFlow collector. This release supports smart logging for DHCP snooping or dynamic ARP inspection violations, IP source guard denied traffic, and ACL traffic permitted or denied on Layer 2 ports (Catalyst 3750 and 3560).
- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate

- VACL Logging to generate syslog messages for ACL denied IP packets (Catalyst 3750 and 3560).
- Support for IPv6 Host and MLD Snooping on the LAN Lite image (Catalyst 2960-S and 2960).
- Support for 802.1x Wake-on-LAN on the LAN Lite image (Catalyst 2960-S and 2960).
- Smart Install enhancements including the ability to manually change a client switch health state from denied to allowed or hold for on-demand upgrades, to remove selected clients from the director database, to allow simultaneous on-demand upgrade of multiple clients, and to provide more information about client devices, including device status, health status, and upgrade status.
- AutoSmartports enhancement to enable auto-QoS on a CDP-capable Cisco digital media player.
- Memory consistency check routine enhancements to detect and correct invalid ternary content addressable memory (TCAM) table entries that can affect switch performance (Catalyst 2960-S).
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.
- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type, as defined in RFC5460 (Catalyst 3750 and 3560).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent (Catalyst 3750 and 3560).
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Support for Multicast Listener Discovery (MLD) snooping on LAN Lite images for efficient distribution of IPv6 multicast data to clients and routers in a switched network (Catalyst 2960-S and 2960).
- NSF IETF mode for OSPFv2—OSPFv2 graceful restart support for IPv4. (Catalyst 3750 and 3560IP services image only)
- NSF IETF mode for OSPFv3—OSPFv3 graceful restart support for IPv6. (Catalyst 3750 and 3560IP services image only)
- Support for the Virtual Router Redundancy Protocol (VRRP) for IPv4, which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address (Catalyst 3750 and 3560).

Minimum Cisco IOS Release for Major Features

Table 7 lists the minimum software release required to support the major features of the Catalyst 3750, 3560, 2960-S, and 2960 switches and the Cisco EtherSwitch service modules.

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Built-in Traffic Simulator using Cisco IOS IP SLAs video operations	12.2(58)SE1	3750, 3560
Cisco Mediatrace support	12.2(58)SE1	3750, 3560
Cisco performance monitor	12.2(58)SE1	3750, 3560
EnergyWise Phase 2.5	12.2(58)SE1	3750, 3560, 2960-S, 2960
Smart logging	12.2(58)SE1	3750, 3560
Protocol storm protection	12.2(58)SE1	3750, 3560, 2960-S, 2960
VACL Logging	12.2(58)SE1	3750, 3560
Smart Install 3.0	12.2(58)SE1	3750, 3560, 2960-S, 2960
Auto Smartports enhancements to enable auto-QoS on a digital media player.	12.2(58)SE1	3750, 3560, 2960-S, 2960
Memory consistency check routines	12.2(58)SE1	2960-S
Call Home support	12.2(58)SE1	3750, 3560, 2960-S, 2960
NTP version 4	12.2(58)SE1	3750, 3560, 2960-S, 2960
DHCPv6 bulk-lease query and DHCPv6 relay source configuration	12.2(58)SE1	3750, 3560
NSF IETF mode for OSPFv2 and OSPFv3 (IP services image)	12.2(58)SE1	3750, 3560
RADIUS, TACACS+, and SSH/SCP over IPv6	12.2(58)SE1	3750, 3560, 2960-S, 2960
VRRP for IPv4	12.2(58)SE1	3750, 3560
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1	3750, 3560, 2960-S, 2960
Auto-QoS enhancements	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
Auto Smartport enhancements including global macros	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
Smart Install enhancements and new features	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
Port ACL improvements	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
CDP and LLDP location enhancements	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
Multi-authentication with VLAN assignment	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
Cisco TrustSec	12.2(55)SE	3750 and 3560
Memory-consistency check routines	12.2(55)SE	3750, 3560, 2975, 2960
Static routing support on SVIs	12.2(55)SE	2975, 2960, and 2960-S
MAC replace to end a session when a host disconnects from a port.	12.2(55)SE	3750, 3560,2975, 2960, 2960-S
DHCP snooping and Option 82 and LLPD-MED in LAN lite image	12.2(55)SE	2960 and 2960-S
Smart Install to allow a single point of management (director) in a network.	12.2(52)SE	3750, 3560,2975, 2960
Support for IP source guard on static hosts.	12.2(52)SE	3750, 3560,2975, 2960

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
AutoSmartPort enhancements (macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros).	12.2(52)SE	3750, 3560,2975, 2960
RADIUS Change of Authorization (CoA).	12.2(52)SE	3750, 3560,2975, 2960
802.1x User Distribution for deployments with multiple VLANs.	12.2(52)SE	3750, 3560,2975, 2960
Critical VLAN with multiple-host authentication.	12.2(52)SE	3750, 3560,2975, 2960
Customizable web authentication enhancement to allow the creation of user-defined pages.	12.2(52)SE	3750, 3560,2975, 2960
Network Edge Access Topology (NEAT) to change the port host mode.	12.2(52)SE	3750, 3560,2975, 2960
VLAN-ID based MAC authentication.	12.2(52)SE	3750, 3560,2975, 2960
MAC move to allow hosts to move across ports on the same switch.	12.2(52)SE	3750, 3560,2975, 2960
3DES and AES with SNMPv3.	12.2(52)SE	3750, 3560,2975, 2960
Hostname support in the option 12 field of DHCPDISCOVER packets.	12.2(52)SE	3750, 3560,2975, 2960
DHCP Snooping enhancement for the circuit-id sub-option.	12.2(52)SE	3750, 3560,2975, 2960
Increased support for LLPD-MED	12.2(52)SE	3750, 3560,2975, 2960
LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE	3750, 3560,2975, 2960
IPv6 QoS trust capability.	12.2(52)SE	3750, 3560
Cisco Medianet to enable intelligent services in the network infrastructure for video applications.	12.2(52)SE	3750, 3560
EEM 3.2 event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.	12.2(52)SE	3750, 3560
Cisco EnergyWise Phase 2 to manage EnergyWise-enabled Cisco devices and non-Cisco end points running EnergyWise agents.	12.2(53)SE1	3750, 3560, 2960
Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement	12.2(50)SE	3750, 3560, 2960
802.1x with open access	12.2(50)SE	3750, 3560, 2960
802.1x authentication with downloadable ACLs and redirect URLs	12.2(50)SE	3750, 3560, 2960
Flexible-authentication sequencing	12.2(50)SE	3750, 3560, 2960
Multiple-user authentication	12.2(50)SE	3750, 3560, 2960
Cisco EnergyWise Phase 1 to manage power usage over PoE devices.	12.2(50)SE	3750, 3560, 2960
Wired location service	12.2(50)SE	3750, 3560, 2960
CPU utilization threshold trap	12.2(50)SE	3750, 3560, 2960
Cisco IOS Configuration Engine (previously the Cisco IOS CNS agent)	12.2(50)SE	3750, 3560, 2960
LLDP-MED network-policy profile time, length, value (TLV)	12.2(50)SE	3750, 3560, 2960

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
RADIUS server load balancing	12.2(50)SE	3750, 3560, 2960
Auto Smartports Cisco-default and user-defined macros	12.2(50)SE	3750, 3560, 2960
SCP attribute support in the CONFIG_COPY MIB, CISCO-AUTH-FRAMEWORK-MIB, CISCO-MAC-AUTH-BYPASS MIBs, LLDP MIB	12.2(50)SE	3750, 3560, 2960
Intermediate System-to-Intermediate System (IS-IS) routing for Connectionless Network Service (CLNS) networks	12.2(50)SE	3750, 3560
Support for Embedded Event Manager Version 2.4.	12.2(50)SE	3750, 3560
IPv6 features in the IP services and IP base images: ACLs; DHCPv6 for the DCHP server, client, and relay device; EIGRPv6; HSRPv6; OSPFv3; RIP; Static routes	12.2(50)SE	3750, 3560
Stack troubleshooting enhancements	12.2(50)SE	3750
802.1x authentication with restricted VLANs	12.2(50)SE	2960
IP source guard	12.2(50)SE	2960
Dynamic ARP inspection	12.2(50)SE	2960
Generic message authentication support with SSH Protocol and compliance with RFC 4256	12.2(46)SE	3750, 3560, 2960
Generic message authentication support	12.2(46)SE	3750, 3560, 2960
Disabling MAC address learning on a VLAN	12.2(46)SE	3750, 3560, 2960
PAgP Interaction with Virtual Switches and Dual-Active Detection	12.2(46)SE	3750, 3560, 2960
DHCP server port-based address allocation	12.2(46)SE	3750, 3560, 2960
IPv6 default router preference (DRP)	12.2(46)SE	3750, 3560, 2960
Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation	12.2(46)SE	3750, 3560
Local web authentication banner	12.2(46)SE	3750, 3560
Support for the CISCO-NAC-NAD and CISCO-PAE MIBs	12.2(46)SE	3750, 3560
Excluding a port in a VLAN from the SVI line-state calculation	12.2(46)SE	3750, 3560
EOT and IP SLAs EOT static route support	12.2(46)SE	3750, 3560
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3750, 3560
HSRP for IPv6 (advanced IP services image)	12.2(46)SE	3750, 3560
DHCP for IPv6 relay, client, server address assignment and prefix delegation (advanced IP services image)	12.2(46)SE	3750, 3560
Embedded event manager (EEM) (IP services image only)	12.2(46)SE	3750, 3560
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA) (LAN base image only)	12.2(46)SE	2960
Monitoring real-time power consumption on a per-PoE port basis	12.2(46)SE	2960

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute	12.2(46)SE	2960
IEEE 802.1x readiness check	12.2(44)SE	3750, 3560, 2960
DHCP-based autoconfiguration and image update	12.2(44)SE	3750, 3560, 2960
Configurable small-frame arrival threshold	12.2(44)SE	3750, 3560, 2960
HTTP and HTTP(s) support over IPV6	12.2(44)SE	3750, 3560, 2960
SNMP configuration over IPv6 transport	12.2(44)SE	3750, 3560, 2960
IPv6 stateless autoconfiguration	12.2(44)SE	3750, 3560, 2960
Flex Link Multicast Fast Convergence	12.2(44)SE	3750, 3560, 2960
Digital optical monitoring (DOM)	12.2(44)SE	3750, 3560
Source Specific Multicast (SSM) mapping	12.2(44)SE	3750, 3560
/31 bit mask support for multicast traffic	12.2(44)SE	3750, 3560
Configuration replacement and rollback	12.2(40)SE	3750, 3560, 2960
Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE	3750, 3560, 2960
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)SE	3750, 3560
Automatic quality of service (QoS) Voice over IP (VoIP)	12.2(40)SE	3750, 3560, 2960
Dynamic voice virtual LAN (VLAN) for MDA-enabled ports	12.2(40)SE	3750, 3560
Internet Group Management Protocol (IGMP) helper	12.2(40)SE	3750, 3560
IP Service Level Agreements (IP SLAs)	12.2(40)SE	3750, 3560
IP SLAs EOT	12.2(40)SE	3750, 3560
Multicast virtual routing and forwarding (VRF) lite	12.2(40)SE	3750, 3560
SSM PIM protocol	12.2(40)SE	3750, 3560
VRF-aware support for HSRP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping	12.2(40)SE	3750, 3560
MLD snooping	12.2(40)SE	2960
IPv6 host	12.2(40)SE	2960
IP phone detection enhancement	12.2(37)SE	3750, 3560, 2960
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE	3750, 3560, 2960
PIM stub routing	12.2(37)SE	3750, 3560
Port security on a PVLAN host	12.2(37)SE	3750, 3560
VLAN aware port security option	12.2(37)SE	3750, 3560, 2960
Auto rendezvous point (auto-RP) for multicast	12.2(37)SE	3750. 3560
VLAN Flex Links load balancing	12.2(37)SE	3750, 3560, 2960
Web Cache Communication Protocol (WCCP)	12.2(37)SE	3750. 3560

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Multidomain authentication (MDA)	12.2(35)SE	3750, 3560
Web authentication	12.2(35)SE	3750, 3560, 2960
MAC inactivity aging	12.2(35)SE	3750, 3560, 2960
Support for IPv6 with Express Setup	12.2(35)SE	3750, 3560
Generic online diagnostics	12.2(35)SE	3560
Stack MAC persistent timer and archive download enhancements	12.2(35)SE	3750
HSRP enhanced object tracking	12.2(35)SE	3750, 3560
OSPF and EIGRP Nonstop forwarding capability (IP services image only)	12.2(35)SE	3750
IPv6 router ACLs for inbound Layer 3 management traffic	12.2(35)SE	3750, 3560
Generic online diagnostics to test the hardware functionality of the supervisor engine	12.2(25)SEE	3750
DHCP Option 82 configurable remote ID and circuit ID	12.2(25)SEE	3750, 3560, 2960
EIGRP stub routing in the IP base image	12.2(25)SEE	3750, 3560
/31 bit mask support for unicast traffic	12.2(25)SEE	3750, 3560
Access SDM templates	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 ACLs	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 Multicast Listener Discovery (MLD) snooping	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
QoS hierarchical policy maps on a port	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
NAC Layer 2 IEEE 802.1x validation	12.2(25)SED	3750, 3560, 2960 Cisco EtherSwitch service modules
NAC Layer 2 IP validation	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x inaccessible authentication bypass.	12.2(25)SED 12.2(25)SEE	3750, 3560 Cisco EtherSwitch service module 2960
IEEE 802.1x with restricted VLAN	12.2(25)SED	3750, 3560, 2960 Cisco EtherSwitch service modules
Budgeting power for devices connected to PoE ports	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEC 12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules| 2960

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Unique device identifier (UDI)	12.2(25)SEC 12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules 2960
VRF Lite	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x with wake-on-LAN	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Nonstop forwarding (NSF) awareness	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
Configuration logging	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Secure Copy Protocol	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Cross-stack EtherChannel	12.2(25)SEC	3750 Cisco EtherSwitch service modules
Private-VLAN on interfaces configured for dynamic ARP inspection	12.2(25)SEB	3750, 3560
IP source guard on private VLANs	12.2(25)SEB	3750, 3560
IEEE 802.1x restricted VLAN	12.2(25)SED	3750, 3560, 2960
IGMP leave timer	12.2(25)SEB 12.2(25)SED	3750, 3560, 2960
IGMP snooping querier	12.2(25)SEA 12.2(25)FX	3750, 3560, 2960
Advanced IP services	12.2(25)SEA	3750, 3560
DSCP transparency	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
VLAN-based QoS[1] and hierarchical policy maps on SVIs[2]	12.2(25)SE	3750, 3560
Device manager	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
IEEE 802.1Q tunneling and Layer 2 protocol tunneling	12.2(25)SE	3750, 3560
Layer 2 point-to-point tunneling and Layer 2 point-to-point tunneling bypass	12.2(25)SE	3750, 3560
SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
Private-VLAN ports on interfaces that are configured for dynamic ARP inspection (IP services image only)	12.2(25)SE	3750, 3560

Table 7 Catalyst 3750, and 3560, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
IP source guard on private VLANs (IP services image only)	12.2(25)SE	3750, 3560
Cisco intelligent power management	12.2(25)SE	3750, 3560
IEEE 802.1x accounting and MIBs (IEEE 8021-PAE-MIB and CISCO-PAE-MIB)	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Dynamic ARP inspection	12.2(20)SE	3750, 3560
Flex Links	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Software upgrade (device manager or Network Assistant only)	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
IP source guard	12.2(20)SE	3750, 3560
Private VLAN (IP services image only)	12.2(20)SE	3750, 3560
SFP module diagnostic management interface	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Switch stack offline configuration	12.2(20)SE	3750
Stack-ring activity statistics	12.2(20)SE	3750
Smartports macros	12.2(18)SE 12.2(25)FX	3750, 3560, 2960
Generic online diagnostics (GOLD)	12.2(25)SEE	3750
Flex Links Preemptive Switchover	12.2(25)SEE	3750, 3560, 2960

1. QoS = quality of service
2. SVIs = switched virtual interfaces

Limitations and Restrictions

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

- Cisco IOS Limitations, page 21
- Device Manager Limitations, page 37

Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3750, and 3560, and 2960 switches and the Cisco EtherSwitch service modules:

Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

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

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

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When the **show interface** privileged EXEC is entered on a port that is running IEEE 802.1Q, inconsistent statistics from ports running IEEE 802.1Q might be reported.

  The workaround is to upgrade to Cisco IOS Release 12.1(20)EA1. (CSCec35100)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When you change a port from a nonrouted port to a routed port or the reverse, the applied auto-QoS setting is not changed or updated when you verify it by using the **show running interface** or **show mls qos interface** user EXEC commands.

  These are the workarounds:

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

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:

  – (Catalyst 3750 switch and Cisco EtherSwitch service modules) When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.

  – (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.

  – (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When dynamic ARP inspection is enabled on a switch or switch stack, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)

- (Catalyst 3750 switches and Cisco EtherSwitch service modules) Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost.

  When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command.

  There is no workaround. (CSCed95822)

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

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

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

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

- (Cisco EtherSwitch service modules) You cannot change the console baud rate by using the switch CLI. The console on the Cisco EtherSwitch service modules only supports three baud rates (9600 b/s, 19200 b/s, and 38400 b/s) and must be set at the bootloader prompt. The switch rejects a CLI command to change the baud rate.

  To change the baud rate, reload the Cisco EtherSwitch service module with the bootloader prompt. You can then change the baud rate and change the speed on the TTY line of the router connected to the Cisco EtherSwitch Service module console.

  There is no workaround. (CSCeh50152)

- When a Catalyst 3750-12S switch boots up, ports 2, 6, and 10 can become active before the Cisco IOS software loading process is complete. Packets arriving at these ports before the switch software is completely loaded are lost. This is a hardware limitation when the switch uses small form-factor pluggable (SFP) modules with copper connections.

  The workaround is to use switch ports other than those specified for redundancy and for applications that immediately detect active links. (CSCeh70503)

- 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
  ```

  (CSCsh12472 [Catalyst 3750 and 3560 switches])

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

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

- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)

- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- When the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as `up` and sometimes as `down`, resulting in conflicts. This status depends on when you respond to the reboot query:

  ```
  Would you like to enter the initial configuration dialog?
  ```

  - After a reboot if you wait until the Line Protocol status of VLAN 1 appears on the console before responding, VLAN 1 line status is always shown as `down`. This is the correct state.
  - The problem (VLAN 1 reporting `up`) occurs if you respond to the query before VLAN 1 line status appears on the console.

  The workaround is to wait for approximately 1 minute after rebooting and until the VLAN 1 interface line status appears on the console before you respond to the query. (CSCsl02680) (Catalyst 3750 and 3560 switches)

- A T-start error message appears after startup under these conditions:
  - Two-link ports on the same switch are connected with a crossover cable.
  - The switch is running Cisco IOS 12.2(50)SE3 or later.

  The workaround is to connect the two ports with a straight-through cable. (CSCsr41271) (Catalyst 3750V2 and Catalyst 3560V2 PoE switches and Cisco Etherswitch service modules only)
- 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)
- When authorization and accounting are enabled on the switch and you use the interface range command to change the configuration on a range of interfaces, the change might cause high CPU utilization and authentication failures.

  The workaround is to disable authorization and accounting or to enter the configuration change for one interface at a time. (CSCsg80238, CSCti76748)

Ethernet

- Link connectivity might be lost between some older models of the Intel Pro1000 NIC and the 10/100/1000 switch port interfaces. The loss of connectivity occurs between the NIC and these switch ports:
  - Ports 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, and 24 of the Catalyst 3750G-24T and 3750G-24TS switches
  - Gigabit Ethernet ports on the Cisco EtherSwitch service modules

  These are the workarounds:
  - Contact the NIC vendor, and get the latest driver for the card.
  - Configure the interface for 1000 Mb/s instead of for 10/100 Mb/s.
  - Connect the NIC to an interface that is not listed here. (CSCea77032)

  For more information, enter *CSCea77032* in the Bug Toolkit at this URL: http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs
- (Cisco EtherSwitch service modules) When a Cisco EtherSwitch service module reloads or the internal link resets, there can be up to a 45-second delay in providing power to PoE devices, depending on the configuration. If the internal Gigabit Ethernet interface on a Cisco EtherSwitch service module connected to the router is configured as a switch port in access mode or in trunk mode, the internal link is not operational until it reaches the STP forwarding state. Therefore, the PoE that comes from the host router is also not available until the internal Gigabit Ethernet link reaches the STP forwarding state. This is due to STP convergence time. This problem does not occur on routed ports.

  If the Cisco EtherSwitch service module is in access mode, the workaround is to enter the **spanning-tree portfast** interface configuration command on the internal Gigabit Ethernet interface. If the service module is in trunk mode, there is no workaround.
- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

If this happens, uneven traffic distribution will happen on EtherChannel ports.

Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

- for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
- for incrementing source-ip traffic, configure load balance method as **src-ip**
- for incrementing dest-ip traffic, configure load balance method as **dst-ip**
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

EtherSwitch Modules

- A duplex mismatch occurs when two Fast Ethernet interfaces that are directly connected on two EtherSwitch service modules are configured as both 100 Mb/s and full duplex *and* as automatic speed and duplex settings. This is expected behavior for the PHY on the Cisco EtherSwitch service modules.

  There is no workaround. (CSCeh35595)

Fallback Bridging

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group.

  The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group.

  The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the **no switchport port-security** interface configuration command. (CSCdz80499)

HSRP

- When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list.

  The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

IP

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out.

  The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

IP Telephony

- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned.

  No workaround is necessary. (CSCea85312)

- (Catalyst 3750 or 3560 PoE-capable switches and Cisco EtherSwitch service modules) The switch uses the IEEE classification to learn the maximum power consumption of a powered device before powering it. The switch grants power only when the maximum wattage configured on the port is less than or equal to the IEEE class maximum. This ensures that the switch power budget is not oversubscribed. There is no such mechanism in Cisco prestandard powered devices.

  The workaround for networks with pre-standard powered devices is to leave the maximum wattage set at the default value (15.4 W). You can also configure the maximum wattage for the port for no less than the value the powered device reports as the power consumption through CDP messages. For networks with IEEE Class 0, 3, or 4 devices, do not configure the maximum wattage for the port at less than the default 15.4 W (15,400 milliwatts). (CSCee80668)

- Phone detection events that are generated by many IEEE phones connected to the switch ports can consume a significant amount of CPU time if the switch ports cannot power the phones because the internal link is down.

  The workaround is to enter the **power inline never** interface configuration command on all the Fast Ethernet ports that are not powered by but are connected to IP phones if the problem persists. (CSCef84975, Cisco EtherSwitch service modules only)

- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the access point as an IEEE Class 1 device.

  The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)

- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

  The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

MAC Addressing

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Management

CiscoWorks is not supported on the Catalyst 3750-24FS switch.

Multicasting

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port.

  There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise.

  The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port.

  There is no workaround. (CSCdy82818)
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN.

  The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)
- (Catalyst 3750 switch stack) If the stack master is power cycled immediately after you enter the **ip mroute** global configuration command, there is a slight chance that this configuration change might be lost after the stack master changes. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands.

  There is no workaround. (CSCea71255)
- (Catalyst 3750 switches and Cisco EtherSwitch service modules) When you enable IP Protocol-Independent Multicast (PIM) on a tunnel interface, the switch incorrectly displays the `Multicast is not supported on tunnel interfaces` error message. IP PIM is not supported on tunnel interfaces.

  There is no workaround. (CSCeb75366)

- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

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

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

  There is no workaround. (CSCee16865)
- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

  After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

  Use one of these workarounds:
  - Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)
- If IP routing is disabled and IP multicast routing is enabled on a switch running Cisco IOS Release 12.2(25)SED, IGMP snooping floods multicast packets to all ports in a VLAN.

  The workaround is to enable IP routing or to disable multicast routing on the switch. You can also use the **ip igmp snooping querier** global configuration command if IP multicast routing is enabled for queries on a multicast router port. (CSCsc02995)

Power

- Non-PoE devices attached to a network might be erroneously detected as an IEEE 802.3af-compliant powered device and powered by the Cisco EtherSwitch service module.

  There is no workaround. You should use the **power inline never** interface configuration command on Cisco EtherSwitch service module ports that are not connected to PoE devices. (CSCee71979)
- When you enter the **show power inline** privileged EXEC command, the out put shows the total power used by all Cisco EtherSwitch service modules in the router. The remaining power shown is available for allocation to switching ports on all Cisco EtherSwitch service modules in the router.

  To display the total power used by a specific EtherSwitch service module, enter the **show power inline** command on the router. This output appears:

  ```
  Router# show power inline
  ```

```
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
INT-PS            0       360.000   121.000         PS1 GOOD   PS2 ABSENT
Interface   Config   Device    Powered    PowerAllocated
---------   ------   ------    -------    --------------
Gi4/0       auto     Unknown  On        121.000 Watts
```

This is not a problem because the display correctly shows the total used power and the remaining power available on the system. (CSCeg74337)

- Entering the **shutdown** and the **no shutdown** interface configuration commands on the internal link can disrupt the PoE operation. If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes.

  The workaround is to enter the **shutdown** and the **no shutdown** interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. (CSCeh45465)

QoS

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue.

  The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)

- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

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

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

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

RADIUS

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

  There is no workaround. (CSCta05071)

Routing

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported.

  There is no workaround. (CSCea52915)

- On a Catalyst 3750 or a Cisco EtherSwitch service module switch stack with a large number of switched virtual interfaces (SVIs), routes, or both on a fully populated nine-member switch stack, this message might appear when you reload the switch stack or add a switch to the stack:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
  Pool: I/O Free: 77124  Cause: Memory fragmentation
  Alternate Pool: None Free: 0  Cause: No Alternate pool
  ```

  This error message means there is a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the **show cef line** user EXEC command and verifying that the line card states are `up` and `sync`.

  No workaround is required because the problem is self-correcting. (CSCea71611)

- (Catalyst 3750 switches and Cisco EtherSwitch service modules) A spanning-tree loop might occur if all of these conditions are true:
  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

  The workaround is to change any one of the listed conditions. (CSCed53633)

Smart Install

- When upgrading switches in a stack, the director cannot send the correct image and configuration to the stack if all switches in the stack do not start at the same time. A switch in the stack could then receive an incorrect image or configuration.

  The workaround is to use an on-demand upgrade to upgrade switches in a stack by entering the **vstack download config** and **vstack download image** commands. (CSCta64962)

- When you upgrade a Smart Install director to Cisco IOS Release 12.2(55)SE but do not upgrade the director configuration, the director cannot upgrade client switches.

  When you upgrade the director to Cisco IOS Release 12.2(55)SE, the workaround is to also modify the configuration to include all built-in, custom, and default groups. You should also configure the tar image name instead of the image-list file name in the stored images. (CSCte07949)

- Backing up a Smart Install configuration could fail if the backup repository is a Windows server and the backup file already exists in the server.

  The workaround is to use the TFTP utility of another server instead of a Windows server or to manually delete the existing backup file before backing up again. (CSCte53737)

- In a Smart Install network, when the director is connected between the client and the DHCP server and the server has options configured for image and configuration, then the client does not receive the image and configuration files sent by the DHCP server during an automatic upgrade. Instead the files are overwritten by the director and the client receives the image and configuration that the director sends.

  Use one of these workarounds:
  - If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.

  - In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director. (CSCte99366)

- In a Smart Install network with the backup feature enabled (the default), the director sends the backup configuration file to the client during zero-touch replacement. However, when the client is a switch in a stack, the client receives the seed file from the director instead of receiving the backup configuration file.

  The workaround, if you need to configure a switch in a stack with the backup configuration, is to use the **vstack download config** privileged EXEC command so that the director performs an on-demand upgrade on the client.

  - When the backup configuration is stored in a remote repository, enter the location of the repository.
  - When the backup file is stored in the director flash memory, you must manually set the permissions for the file before you enter the **vstack download config** command. (CSCtf18775)

- If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point.

  There is no workaround. (CSCtg98656)

- When a Smart Install director is upgrading a client switch that is not Smart Install-capable (that is, not running Cisco IOS Release 12.2(52)SE or later), the director must enter the password configured on the client switch. If the client switch does not have a configured password, there are unexpected results depending on the software release running on the client:

  - When you select the NONE option in the director CLI, the upgrade should be allowed and is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.
  - When you enter any password in the director CLI, the upgrade should not be allowed, but it is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.

  There is no workaround. (CSCth35152)

SPAN and RSPAN

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the **replicate** option. For a remote SPAN session, there is no workaround.

  This is a hardware limitation and only applies to these switches (CSCdy72835):

  - 3560-24PS
  - 3560-48PS
  - 3750-24PS
  - 3750-48PS
  - 3750-24TS
  - 3750-48TS
  - 3750G-12S

  - 3750G-24T
  - 3750G-24TS
  - 3750G-16TD
  - Cisco EtherSwitch service modules

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

  This is a hardware limitation and only applies to these switches (CSCdy81521):

  - 3560-24PS
  - 3560-48PS
  - 3750-24PS
  - 3750-48PS
  - 3750-24TS
  - 3750-48TS
  - 3750G-12S
  - 3750G-24T
  - 3750G-24TS
  - 3750G-16TD
  - Cisco EtherSwitch service modules

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

  This is a hardware limitation and only applies to these switches (CSCea72326):

  - 3560-24PS
  - 3560-48PS
  - 3750-24PS
  - 3750-48PS
  - 3750-24TS
  - 3750-48TS
  - 3750G-12S
  - 3750G-24T
  - 3750G-24TS
  - 3750G-16TD
  - Cisco EtherSwitch service modules

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded.

  There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

- On Catalyst 3750 switches running Cisco IOS Release 12.1(14)EA1 and later, on Catalyst 3560 switches running Cisco IOS release 12.1(19)EA1 or later, or on Cisco EtherSwitch service modules, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned.

  There is no workaround. (CSCeb23352)

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Stacking (Catalyst 3750 or Cisco EtherSwitch service module switch stack only)

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)

- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual bootup is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots.

  There is no workaround. (CSCec36644)

- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mb/s egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch (such as a Catalyst 3750-24TS or 3750-48TS switch) than if it is on a Gigabit Ethernet switch (such as a Catalyst 3750G-24T or 3750G-24TS switch).

  There is no workaround. (CSCed00328)

- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost.

  The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)

- When the **switchport** and **no switchport** interface configuration commands are entered more than 20,000 times on a port of a Catalyst 3750 switch or on a Cisco EtherSwitch service module, all available memory is used, and the switch halts.

There is no workaround. (CSCed54150)

- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master re-election occurs on one of the Catalyst 3750 or Cisco EtherSwitch service module default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master re-election cannot complete.

  The workaround is to complete the MAC address update by entering the **clear arp** privileged EXEC command. (CSCed62409)

- When a Catalyst 3750 switch or Cisco EtherSwitch service module is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded.

  There is no workaround. (CSCed70894)

- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the IP base image and the old stack master was running the IP services image.

  Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the IP services image or the IP base image:

  – If the stack master is running the IP services image, all stack members have private VLAN enabled.

  – If the stack master is running the IP base image, all stack members have private VLAN disabled.

  This occurs after a stack master re-election when the previous stack master was running the IP services image and the new stack master is running the IP base image. The stack members are configured with private VLAN, but any new switch that joins the stack will have private VLAN disabled.

  These are the workarounds. Only one of these is necessary:

  – Reload the stack after an IP services image to IP base image master switch change (or the reverse).

  – Before an IP services image-to-IP base image master switch change, delete the private-VLAN configuration from the existing stack master. (CSCee06802)

- Port configuration information is lost when changing from **switchport** to **no switchport** modes on Catalyst 3750 switches.

  This is the expected behavior of the offline configuration (provisioning) feature. There is no workaround. (CSCee12431)

- When connected to the router through an auxiliary port in a session to a Cisco EtherSwitch service module, the service module session fails when you enter the **shutdown** and the **no shutdown** interface configuration commands on the service module router interface.

  These are the workarounds:

  – Reload the router.

  – Connect to the router through the console port, and open a session to the service module. (CSCeh01250) (Cisco EtherSwitch service modules)

- If one switch in a stack of Catalyst 3750 switches requires more time than the other switches to find a bootable image, it might miss the stack master election window. However, even if the switch does not participate in the stack master election, it will join the stack as a member.

  The workaround is to copy the bootable image to the parent directory or first directory. (CSCei69329)

- When the path cost to the root bridge is equal from a port on a stacked root and a port on a non stack root, the BLK port is not chosen correctly in the stack when the designated bridge priority changes. This problem appears on switches running in PVST, Rapid-PVST, and MST modes.

  The workaround is to assign a lower path cost to the forwarding port. (CSCsd95246)

- When a stack of 3750 switches is configured with a Cross-Stack EtherChannel and one of the physical ports in the EtherChannel has a link-up or a link-down event, the stack might transmit duplicate packets across the EtherChannel. The problem occurs during the very brief interval while the switch stack is adjusting the EtherChannel for changing conditions and adapting the load balance algorithm to the new set of active physical ports.

  This can but does not always occur during link flaps and does not last for more than a few milliseconds. This problem can happen for cross-stack EtherChannels with the mode set to ON or LACP.

  There is no workaround. No manual intervention is needed. The problem corrects itself within a short interval after the link flap as all the switches in the stack synchronize with the new load-balance configuration. (CSCse75508)

- 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 being entered, 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)

- The error message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:

  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.

  You can use one of these workarounds:

  - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
  - Remove and reconfigure the VLAN. (CSCsi26444)

- In a mixed stack of Catalyst 3750 switches and Catalyst 3750-E switches, when the stack reloads, the Catalyst 3750-E might not become stack master, even it has a higher switch priority set.

  The workaround is to check the flash. If it contains many files, remove the unnecessary ones. Check the lost and found directory in flash and if there are many files, delete them. To check the number of files use the **fsck flash:** command. (CSCsi69447)

- A stack member switch might fail to bundle Layer 2 protocol tunnel ports into a port channel when you have followed these steps:

  1. You configure a Layer 2 protocol tunnel port on the master switch.
  2. You configure a Layer 2 protocol tunnel port on the member switch.
  3. You add the port channel to the Layer 2 protocol tunnel port on the master switch.

4. You add the port channel to the Layer 2 protocol tunnel port on the member switch.

After this sequence of steps, the member port might stay suspended.

The workaround is to configure the port on the member switch as a Layer 2 protocol tunnel and at the same time also as a port channel. For example:

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# channel-group 1 mode on
```

(CSCsk96058) (Catalyst 3750 switches)

- After a stack bootup, the spanning tree state of a port that has IEEE 802.1x enabled might be blocked, even when the port is in the authenticated state. This can occur on a voice port where the Port Fast feature is enabled.

  The workaround is to enter a **shutdown** interface configuration command followed by a **no shutdown** command on the port in the blocked state. (CSCsl64124)

- When a switch stack is running 802.1x single host mode authentication and has filter-ID or per-user policy maps applied to an interface, these policies are removed if a master switchover occurs. Even though the output from the **show ip access-list** privileged EXEC command includes these ACLs, the policies are not applied.

  The workaround it to enter a **shutdown** and then a **no shutdown** interface configuration command on the interface. (CSCsx70643) (Catalyst 3750 switch)

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

  There is no workaround.(CSCth00938) (Catalyst 3750 and 2960-S switches)

Trunking

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface.

  There is no workaround. (CSCdz33708)

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y.

  There is no workaround. (CSCdz42909).

- If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch stack is on a different switch than the alternate root port, changing the port priority of the designated ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch stack.

  There is no workaround. (CSCea40988)

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

  There is no workaround. (CSCec35100).

VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- (Catalyst 3750 or 3560 switches) A CPUHOG message sometimes appears when you configure a private VLAN. Enable port security on one or more of the ports affected by the private VLAN configuration.

  There is no workaround. (CSCed71422)

- (Catalyst 3750) When you apply a per-VLAN quality of service (QoS), per-port policer policy-map to a VLAN Switched Virtual Interface (SVI), the second-level (child) policy-map in use cannot be re-used by another policy-map.

  The workaround is to define another policy-map name for the second-level policy-map with the same configuration to be used for another policy-map. (CSCef47377)

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

  The workaround is to configure the burst interval to more than 1 second. (CSCse06827, Catalyst 3750 switches only)

- 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)

- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

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 launch.

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

Important Notes

Switch Stack Notes

- Always power off a switch before adding or removing it from a switch stack.
- Catalyst 3560 switches do not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because these switches share common code with other switches that do support stacking.
- Catalyst 3750 switches running Cisco IOS Release 12.2(25)SEB are compatible with Cisco EtherSwitch service modules running Cisco IOS Release 12.2(25)EZ. Catalyst 3750 switches and Cisco EtherSwitch service modules can be in the same switch stack. In this switch stack, the Catalyst 3750 switch or the Cisco EtherSwitch service module can be the stack's active switch.

Cisco IOS Notes

- The IEEE 802.1x feature in Cisco IOS Release 12.1(14)EA1 and later is not fully backward-compatible with the same feature in Cisco IOS Release 12.1(11)AX. If you are upgrading a Catalyst 3750 switch running Cisco IOS Release 12.1(11)AX that has IEEE 802.1x configured, you must re-enable IEEE 802.1x after the upgrade by using the **dot1x system-auth-control** global configuration command. This global command does not exist in Cisco IOS Release 12.1(11)AX. Failure to re-enable IEEE 802.1x weakens security because some hosts can then access the network without authentication.
- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(18)SE and later. In Cisco IOS Release 12.1(19)EA and earlier, both of these command pairs disabled logging to the console:
  - the **no logging on** and then the **no logging console** global configuration commands
  - the **logging on** and then the **no logging console** global configuration commands

  In Cisco IOS Release 12.2(18)SE and later, you can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)
- In Cisco IOS Release 12.2(25)SEC for the Catalyst 3750 and 3560 switches and in Cisco IOS Release 12.2(25)SED for the Catalyst 2960 switch, the implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.
- 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, check that there is network connectivity between the switch and the ACS. You should also check 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)SE (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

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

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

Device Manager Notes

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese
- The Legend on the device manager incorrectly includes the 1000BASE-BX SFP module.
- We recommend this browser setting to speed up 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.

  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** {**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 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

Unless otherwise noted, these caveats apply to the Catalyst 3750, 3560, 2960-S, and 2960 switches and to Cisco EtherSwitch service modules:

- CSCtg35226 (Catalyst 3750 switches)

  Cisco Network Assistant displays the LED ports with a light blue color for all switches in a stack that have the Catalyst 3750G-48PS switch as part of the stack.

  There is no workaround.

- CSCtg98453

  When you make port security changes on an interface, such as configuring aging time, violations, or aging type, error messages and tracebacks might appear.

  There is no workaround.

- CSCti30313 (Catalyst 2960 and 2960-S switches)

  The output from the **show sdm prefer lanbase-routing** privileged EXEC command shows some incorrect values. The corrected values are:

```
number of IPv4 unicast routes:                   4.25K should be: 0.75K
    number of directly-connected IPv4 hosts:       4K  should be: 0.75K
    number of indirect IPv4 routes:                0.256    should be 16
```

  There is no workaround.

- CSCtj97806 (Catalyst 3750 and 3560 switches)

  Mediatrace does not report statistics on the initiator under these conditions:

  - The responder is a mixed switch stack with a Catalyst 3750 as the master switch
  - The ingress interface on the responder from the initiator is on a member switch.

  The workaround is to ensure that the mediatrace ingress and egress connections are on the stack master or to configure a Catalyst 3750-E or 3750-X as the stack master and then reload the switch stack.

- CSCtl32991

  Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue.

Note This does not occur when packets are routed through the switch to another destination.

  There is no workaround.

- CSCtl60247

When a switch or switch stack running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

There is no workaround.

- CSCtl81217 (Catalyst 3750 and 3560)

  When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, if the switch reloads, the interface loses some RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.

  There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:

  ip rip authentication mode

  ip rip key-chain

- CSCto41442 (Catalyst 3750)

  When you configure OSPFv3 graceful restart on a stack of switches with more than one OSPF area and you use the **router-id** *ip-address* router configuration command to configure a fixed router ID, if there is a switchover of the stack master switch, OSPFv3 graceful restart might be terminated.

  The workaround, if possible, is to not use the **router-id** command to configure a fixed router ID with OSPFv3 graceful restart.

- CSCts52797 (Catalyst 2960)

  A Catalyst 2960 with 64Mb of DRAM might display low memory on the console after you upgrade the switch to 12.2(58)SE or later.

  The workaround is to limit the memory that is used by different features on the switch if this release is required. You can reduce memory usage by minimizing the number of trunk ports and VLANs in use on the switch.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- CSCtj83964 (Catalyst 3750 and 3560 switches)

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

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

- CSCtl51859

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

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

Caveats Resolved in Cisco IOS Release 12.2(58)SE2

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCtq01926

  When you configure a port to be in a dynamic VLAN by entering the **switchport access vlan dynamic** interface configuration command on it, the switch might reload when it processes ARP requests on the port.

  The workaround is to configure static VLANs for these ports.

- CSCtq32728 (Catalyst Switches 2960, 2960-S and 2960-SM)

  Fallback web authentication does not work.

  The workaround is to downgrade to Cisco IOS Release 12.2(55)SE2.

- CSCtq82410 (Catalyst Switch 3560)

  The switch fails when a port channel is created with a WS-6708-GE-TX line card on the other end of the port channel.

  The workaround is to downgrade to a release earlier than Cisco IOS Release 12.2(55)SE.

- CSCsq44330 (Catalyst Switch 3750)

  Use the **vlan dot1q tag native** global configuration command to configure the edge switch so that all packets going out an IEEE 802.1Q trunk, including the native VLAN, are tagged. If the switch is configured to tag native VLAN packets on all IEEE 802.1Q trunks, the switch accepts untagged packets, but sends only tagged packets.

Caveats Resolved in Cisco IOS Release 12.2(58)SE1

- CSCta39338 (Catalyst 3560 and 2960)

When you globally enable UDLD by entering the **udld** {**aggressive | enable | message time** *message-timer-interval*} global configuration command, UDLD is now enabled only on fiber optic ports and on dual-purpose ports operating as fiber optic interfaces. It is not enabled on copper ports or dual-purpose ports operating as copper interfaces. For the **udld** global configuration command to enable UDLD on dual-purpose ports that have a small form-factor pluggable (SFP) module connected, you must explicitly configure the interface media type as SFP by entering the **media-type sfp** interface configuration command.

- CSCtc72940 (Catalyst 3750)

  When you reload a stack master, the **ip vrf forwarding** command does not appear in the running configuration, which causes AAA authentication to fail. This issue does not occur with standalone switches.

  The workaround is to reenter the **ip vrf forwarding** command.

- CSCtf21181 (Catalyst 3750 switches)

  A switch stack configured as a multicast router has a hardware programming error. Some multicast streams are not forwarded to a receiver while other streams from the same source are forwarded correctly. The unforwarded streams are Layer 2 forwarded by the stack on the same VLAN on which they were received to the multicast designated router for the VLAN.

  The workaround is to use the **clear ip mroute** privileged EXEC command to resolve the hardware programming error.

- CSCtg00542 (Catalyst 3750 and 3560)

  A Link Aggregation Control Protocol (LACP) bundle takes up to 70 seconds to form when NetFlow sampling is enabled.

  The workaround is to disable NetFlow sampling.

- CSCtg11547

  When you configure a switch to send messages to a syslog server in a VPN Routing and Forwarding (VRF) instance, the messages are not sent to the server.

  The workaround is to remove the VRF configuration.

- CSCtg71149

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

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

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

- CSCth24278 (Catalyst 2960-S switches)

  The CPU utilization on the switch remains high (50 to 60 percent) when the switch is not being accessed by a telnet or a console session. When you telnet or console into the switch, the CPU utilization goes down.

  There is no workaround.

- CSCth44403 (Catalyst 3750 and 3560)

  When you connect a switch as a VLAN Trunk Protocol (VTP) client to a Catalyst 4000 switch configured as a VTP client or server and the VTP database contains more than 512 VLANs, the database is not correctly updated.

  The workaround is to connect the VTP client directly to a Catalyst 6500 VTP server.

- CSCth71862 (Catalyst 3750 and 2960-S)

  A host switch connected to a stack member switch can download a downloadable access control list (dACL) with more than 13 access control entries, but the dACL is not applied to an interface.

  There is no workaround.

- CSCti20222 (Catalyst 3750 and 2960-S)

  On a stack member, the **show interface** command output incorrectly displays a media-type setting.

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

- CSCti37197

  Enabling the Cisco Discovery Protocol (CDP) on a tunnel interface causes the switch to fail when a a CDP packet is received on the interface.

Note Tunnels are not supported on these platforms.

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

- CSCti45352

  When a FlexLinks backup interface is configured on a member switch in a switch stack, the backup interface incorrectly shows that all VLANs are in the forwarding state.

  The workaround is to use the **show interface trunk** interface configuration command to display the status of the backup link.

- CSCti61123 (Catalyst 2960-S switch)

  A Catalyst 29560-S switch downlink port cannot connect to the uplink port of a Catalyst compact switch.

  The workaround is to configure the speed to 100 Mb/s on both ports.

- CSCti69813 (Catalyst 2960-S switch)

  When a new member switch with a different SDM template than that of the master switch is added to a stack, it does not reload with the SDM template of the stack master switch and does not display an SDM mismatch condition.

  There is no workaround.

- CSCti78365

  The config.text.backup file is present after the switch is restored to the factory defaults.

  There is no workaround.

- CSCti95834

  When you enter the **ipv6 traffic-filter** interface configuration command, it might not filter traffic as expected, and it might allow traffic to pass through.

  There is no workaround.

- CSCti95979 -R (Catalyst 3750 and 2960-S)

  QoS ACL commands might appear differently in the running configuration after the master switch is reloaded or removed from the stack. The functionality of the commands remains the same.

  There is no workaround.

- CSCtj03875

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

  There is no workaround.

- CSCtj25488 (Catalyst 3750 switch)

  Two stacks that have members with fiber SFP modules are connected in a cross-stack EtherChannel with this configuration:

  - Layer 3 EtherChannels
  - EtherChannel **on** mode

  If a member in one stack is reloaded, this error message appears on a member switch port in the other stack and the port is error disabled.

  ```
  %PLATFORM_PM-3-INTVLANINUSE: internal vlan-id 1012 allocated for interface Gi2/0/2 is
  still in use (3750-b-2)-Traceback= 173E7F0 198F40C 176DA04 1774E70 173FBDC 1744574
  16C9C28 17C65C4 17C67D8 1BB7308 1BADD78 (3750-b-2)
  ```

  The workaround is to configure Layer 2 EtherChannels with SVIs and to use the EtherChannel **Active** mode.

- CSCtj37604 (Catalyst 2960-S switch)

  A switch stack reloads when you enter the **ip routing** global configuration command.

  The workaround is to use the **no ip routing** global configuration command to disable IP routing.

- CSCtj52611 (Catalyst 2960-S switch)

  When the destination IP address matches the default route, the switch does not forward traffic.

  The workaround is to use a specific static route such as

  ```
  ip route 0.0.0.0 128.0.0.0
  ip route 192.168.0.0 128.0.0.0
  ```

- CSCtj75471

  When a spanning-tree bridge protocol data unit (BPDU) is received on an 802.1Q trunk port and has a VLAN ID is greater than or equal to 4095, the spanning-tree lookup process fails.

  There is no workaround.

- CSCtj83697 (Catalyst 2960-S switch)

  When the Ethernet management port speed is 10 Mb/s and the link between the switch and its peer is up, IP ping fails.

  The workaround is to set the speed to 100 Mb/s.

- CSCtj84257 (Catalyst 2960-S switch)

  When a GLC-FE-100FX SFP module port is in full-duplex mode, it changes to half-duplex mode after you enter the **shutdown** and the **no shutdown** interface configuration commands or after the link between the switch and another device fails and then comes up.

  The workaround is to enter the **no duplex** and the **duplex full** interface configuration commands.

- CSCtj88040 (Catalyst 3750 and 2960-S)

  When a stack is running per-VLAN spanning-tree plus (PVST+) and you create a VLAN, the STP topology change resets the aging time for all members and ages out all the MAC addresses for the new VLAN. If a cookie for the new VLAN on the member is not created when the master sends the member an HRPC message to update the aging timer, the member changes the aging time for VLAN 1 to that set during the topology change.

  After the topology change, the aging time for the new VLAN is reset to that before the STP topology changed. However, the aging time for VLAN 1 does not change. The MAC addresses learned on VLAN 1 and on the member switch ports age out before aging time for the new VLAN.

  The workaround is to disable STP before creating a new VLAN in the stack.

- CSCtj88307

  When you enter the **default interface**, **switchport**, or **no switchport** interface configuration command on the switch, this message appears: *`EMAC phy access error, port 0, retrying.....`*

  There is no workaround.

- CSCtj95182

  When you use a network scanner to check network devices for security issues, the CPU usage increases.

  There is no workaround.

- CSCtk11275

  On a switch running Cisco IOS Release 12.2(55)SE with the **parser config cache interface** global configuration command in the configuration, when you use the CISCO-MAC-NOTIFICATION-MIB to enable the SNMP MAC address notification trap, the trap is enabled, but the trap setting does not appear in the switch configuration.

  The workaround is to remove the **parser config cache interface** command from the configuration.

- CSCtk13113

  The CPU usage on a standalone switch varies as the switch updates the running configuration.

  There is no workaround.

- CSCtk32638 (Catalyst 3750 switch)

  When the switch stack elects a new stack master, by default the MAC address of the new master becomes the stack MAC address. Configuring a persistent MAC address sets a delay after stack master change before the stack master MAC address change. A timer value of 0 means that the MAC address of the current master is used indefinitely.

  When you enter the **stack-mac persistent timer 0** global configuration command on a stack and the master switch is not the original owner of the stack MAC address, ports on member switches do not go through Rapid Spanning Tree Protocol (STP) transitions directly into the forwarding state.

  The workaround is to not use the **stack-mac persistent timer 0** command on the switch stack.

- CSCtk54457 (Catalyst 2960-S switch)

  On Catalyst 2960-S, 3560-X, and 3750-X switches, some SFP+ module ports do not work correctly with 1 Gigabit SFP modules when the speed for the port and for the connected device is set to **nonegotiate**. This occurs only on some ports and some SKUs.

  The workaround is to set the speed on the SFP interface to autonegotiate by entering the **speed auto** interface configuration command.

- CSCtk64420 (Catalyst 2960-S switch)

  When a Catalyst 2960-S FlexStack with four switches is connected to a Catalyst 3750 switch, and devices in the same VLAN are connected to the Catalyst 2960-S switches but a device in another VLAN is connected to the Catalyst 3750, if you recycle power on one of the Catalyst 2960-S switches, connected devices can lose packets.

  There is no workaround.

- CSCtk98539 (Catalyst 2960-S switch)

  When quality of service (QoS) is disabled on a switch, packet fragments might be dropped when more traffic is exiting a port than the bandwidth allows. The port can become oversubscribed because fragments are sent to an incorrect egress queue that has fewer buffers.

  The workaround is to enable QoS by entering the **mls qos** global configuration command.

- CSCtl11469 (Catalyst 3750, 3560, 2960, and 2960-S PoE switches)

  The SNMP Get action does not work correctly on Cisco IOS Releases 12.2(46)SE and 12.2(53)SE with the pethMainPseOperStatus operation.

  The workaround is to use the SNMP Walk utility instead of SNMP Get.

- CSCtl42740

  When 802.1x MAC authentication bypass with multidomain authentication and critical VLAN are enabled on an interface on a switch running Cisco IOS Release 12.2(53)SE or later, if the switch loses connectivity with the AAA server, the switch might experience high CPU usage and show these messages:

  ```
  AUTH-EVENT (Gi0/15) Received clear security violation
  AUTH-EVENT (Gi0/15) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on port
  GigabitEthernet0/15
  ```

  There is no workaround.

- CSCtl57976 (Catalyst 2960-S switches)

  If the startup configuration file is empty on the master switch and Multiple Spanning Tree Protocol (MSTP) is configured on the switch stack, the stack fails and reloads when you enter the **config replace nvram:startup-config** user EXEC command.

  The workaround is to ensure that a valid startup configuration file exists on the master switch.

- CSCtl80678

  The port manager callback might cause more than 90% CPU usage for up to 20 minutes under these conditions:

  - Link comes up simultaneously on multiple dot1q trunk ports.
  - VLAN Trunking Protocol (VTP) pruning is enabled.

  The workaround is to disable VTP pruning.

- CSCto62631

  A switch running Cisco IOS Release 12.2(58)SE might reload if:

  - SSH version 2 is configured on the switch, and
  - a customized login banner was configured by using the **banner login** *message* global configuration command

  Use one of these workarounds:

  - Disable the login banner by entering the **no login banner** command.

- Disable SSH on the switch.
- Downgrade to a software version prior to Cisco IOS Release 12.2(58)SE.

Documentation Updates

Note The "Supported MIBs" appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Control Plane Protection

Catalyst 2960-S switches internally support up to 16 different control plane queues. Each queue is dedicated to handling specific protocol packets and is assigned a priority level. For example, STP, routed, and logged packets are sent to three different control plane queues, which are prioritized in corresponding order, with STP having the highest priority. Each queue is allocated a certain amount of processing time based on its priority. The processing-time ratio between low-level functions and high-level functions is allocated as 1-to-2. Therefore, the control plane logic dynamically adjusts the CPU utilization to handle high-level management functions as well as punted traffic (up to the maximum CPU processing capacity). Basic control plane functions, such as the CLI, are not overwhelmed by functions such logging or forwarding of packets.

Update to the Catalyst 3750 Software Configuration Guide

In the "Managing Switch Stacks" chapter, this information is added.

In a mixed stack that has Catalyst 3750-X, Catalyst 3750-E, and Catalyst 3750 switches, we recommend that a Catalyst 3750-X switch be the stack's active switch and that all stack members run Cisco IOS Release 12.2(53)SE2 or later. The Catalyst 3750 image is on the Catalyst 3750-X and 3750-E switches to simplify switch management.

To upgrade the stack, use the **archive download-sw** privileged EXEC command to download images to the active switch. For example, use the **archive download-sw /directory tftp://10.1.1.10/ c3750-ipservicesk9-tar.122-55.SE1.tar c3750e-universalk9-tar.122-55.SE1.tar** command to specify a directory, following the command with the list of tar files to download for the members.

- The c3750-ipservicesk9-tar.122-55.SE1.tar is for the Catalyst 3750 members.
- The c3750e-universalk9-tar.122-55.SE1.tar is for the Catalyst 3750-X and 3750-E members.

You can display the file list that is in the flash memory:

```
Switch# dir flash: c3750e-universalk9-tar.122-55.SE1
Directory of flash:/c3750e-universalk9-tar.122-55.SE1/

   5  -rwx   14313645   Mar 1 1993 00:13:55 +00:00   C3750e-universalk9-tar.122-55.SE1.tar
   6   drwx  5632       Mar 1 1993 00:15:22 +00:00   html
 443  -rwx   444        Mar 1 1993 00:15:58 +00:00   info
 444  -rwx   14643200   Mar 1 1993 00:04:32 +00:00   c3750-ipservicesk9-tar.122-55.SE1.tar
```

Update to the Catalyst 2960 and 2960-S Software Configuration Guide

In the "Configuring SDM Templates" chapter, the LAN base routing template has incorrect values. The corrected values are:

```
number of IPv4 unicast routes:                    4.25K should be: 0.75K
    number of directly-connected IPv4 hosts:        4K  should be: 0.75K
    number of indirect IPv4 routes:                 0.256    should be 16
```

Updates to the System Message Guides

New System Messages

Error Message `IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]`

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-ARP: vlan [dec] (port [chars]) denied arp ip [inet] -> [inet], [dec] packet[chars]`

Explanation A packet from the virtual LAN (VLAN) that matches the VLAN access-map (VLMAP) log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-L4: vlan [dec] (port [chars]) denied [chars] [inet]([dec]) -> [inet]([dec]), [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the second [chars] is the protocol, the first [inet] is the source IP address, the second [dec] is the source port, the second [inet] is the destination IP address, the third [dec] is the destination port, the fourth [dec] denotes the number of packets, and the third [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-IGMP: vlan [dec] (port [chars]) denied igmp [inet] -> [inet] ([dec]), [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] is the Internet Group Management Protocol (IGMP) message type, the third [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-ICMP: vlan [dec] (port [chars]) denied icmp [inet] -> [inet] ([dec]/[dec]), [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] is the Internet Control Message Protocol (ICMP) message type, the third [dec] is the ICMP message code, the fourth [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-IP: vlan [dec] (port [chars]) denied ip protocol=[dec] [inet] -> [inet], [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the second [dec] is the protocol number, the first [inet] is the source IP address, the second [inet] is the destination IP address, the third [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `HARDWARE-2-PSU_THERMAL_WARNING: PSU [chars] temperature has reached warning threshold`

Explanation The switch power supply unit (PSU) temperature sensor value has reached the warning level. The external temperature is high. [chars] is the power supply.

Recommended Action Reduce the temperature in the room. (The switch functions normally until the temperature reaches the critical level.)

Error Message `HARDWARE-1-PSU_THERMAL_CRITICAL: PSU [chars] temperature has reached critical threshold`

Explanation The switch PSU temperature sensor value has reached the critical level, and the switch cannot function normally. The external temperature is very high. [chars] is the power supply.

Recommended Action Immediately reduce the room temperature.

Error Message `HARDWARE-5-PSU_THERMAL_NORMAL: PSU [chars] Temperature is within the acceptable limit`

Explanation The switch PSU temperature sensor value is within normal limits. [chars] is the power supply.

Recommended Action No action is required.

Error Message `HARDWARE-2-THERMAL_WARNING: Temperature has reached warning threshold`

Explanation The switch temperature sensor value has reached the warning level. The external temperature is high.

Recommended Action Reduce the room temperature. (The switch functions normally until the temperature reaches the critical level.)

Error Message `AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]`

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

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

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

Recommended Action No action is required.

Modified System Messages

Error Message `AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]`

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message `AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])`

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Error Message `EOU-6-IDENTITY_MATCH: IP=[inet]| PROFILE=EAPoUDP| POLICYNAME=[chars]| AUDITSESSID=[chars]`

Explanation The router has found the specifed host under the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile. [inet] is the host IP address, the first [chars] is the enforced policy, and the second [chars] is the session ID.

Recommended Action If you do not want the host to be exempt from authentication, remove its entry from the EAPoUDP identity profile.

Error Message `EOU-5-RESPONSE_FAILS: Received an EAP failure response from AAA for host=[inet]| AUDITSESSID=[chars]`

Explanation The router received an EAP failure response from authentication, authorization, and accounting (AAA). The host credentials were not validated. [inet] is the host, and [chars] is the session ID.

Recommended Action Check for causes of unsuccessful AAA validation of host credentials.

Error Message `EOU-6-SESSION: IP=[inet]| HOST=[chars]| Interface=[chars]| AUDITSESSID=[chars]`

Explanation An entry for the host was created or deleted on the specified interface. [inet] is the host IP address, the first [chars] is the host identifier, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `EOU-4-VERSION_MISMATCH: HOST=[inet]| Version=[dec]| AUDITSESSID=[chars]`

Explanation A mismatch in the EAPoUDP versions was detected from the host. [inet] is the host identifier, [dec] is the EAPoUDP version, and [chars] is the session ID.

Recommended Action Check EAPoUDP versions on peers.

Error Message `EOU-6-POSTURE: IP=[inet]| HOST=[chars]| Interface=[chars]|AUDITSESSID=[chars]`

Explanation The posture validation status for the host. [inet] is the host IP address, the first [chars] is the host identfier, the second [chars] is the host interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `EOU-6-AUTHTYPE: IP=[inet]| AuthType=[chars]| AUDITSESSID=[chars]`

Explanation The authentication type for the host. [inet] is the host IP address, the first [chars] is the authentication type, and the second [chars] is the session ID.

Recommended Action No action is required.

Error Message `EOU-4-UNKN_EVENT_ERR: UNKNOWN Event for  HOST=[inet]| Event=[dec]| AUDITSESSID=[chars]`

Explanation Unknown message for the EAPoUDP process. [inet] is the host identifier, [dec] is the event identifier, and [chars] is the session ID.

Recommended Action File a DDTS with Cisco.

Error Message `EOU-5-AAA_DOWN: AAA unreachable. METHODLIST=[chars]| HOST=[inet]| POLICY=[chars].| AUDITSESSID=[chars]`

Explanation The AAA servers defined by the method list cannot be reached by the host and the applied policy. The first [chars] is the method list identifer, [inet] is the host identifier, the second [chars] is the policy, and the third [chars] is the session ID.

Recommended Action Check the possible causes for unreachable AAA servers.

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

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

Recommended Action No action is required.

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

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

Recommended Action No action is required.

Deleted System Messages

Error Message `IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST`

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

Update to the Catalyst 3560 and Catalyst 2960 Hardware Installation Guides

In the "Switch Installation (24- and 48-Port Switches)" chapter, the note in the "Connecting to a Dual-Purpose Port" section is incorrect. The correct information is:

Note By default, the switch automatically selects the interface type the first time a port links up. For subsequent links, you must use the **media-type** interface configuration command to manually configure either the RJ-45 connector or the SFP module connector. For more information, see the command reference.

Updates to the Catalyst 2960 Hardware Installation Guide

Cisco Ethernet Switches are equipped with cooling mechanisms, such as fans and blowers. However, these fans and blowers can draw dust and other particles, causing contaminant buildup inside the chassis, which can result in a system malfunction.

You must install this equipment in an environment as free as possible from dust and foreign conductive material (such as metal flakes from construction activities).

This applies to all Cisco Ethernet switches except for these compact models:

- Catalyst 2960-8TC switch—8 10/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
- Catalyst 2960G-8TC switch—7 10/100/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)

Update to the 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*.

Update to the Catalyst 2960-S Switch Getting Started Guide

This correction applies to the French, Italian, German, Spanish, Japanese, and simplified Chinese versions of the getting started guide:

In the "Unpacking the Switch" section, four number-8 Phillips flat-head screws (48-0655-01) are included with the switch.

Related Documentation

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

These documents provide complete information about the Catalyst 3750, 3560, 2975, 2960-S and 2960 switches and the Cisco EtherSwitch service modules and are available at Cisco.com:

http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/ps10081/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

These documents provide complete information about the Catalyst 3750 switches and the Cisco EtherSwitch service modules:

- *Catalyst 3750 Switch Software Configuration Guide*
- *Catalyst 3750 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*
- *Catalyst 3750 Switch Hardware Installation Guide*
- *Catalyst 3750 Getting Started Guide*
- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*

These documents provide complete information about the Catalyst 3750G Integrated Wireless LAN Controller Switch and the integrated wireless LAN controller and are available at cisco.com:

- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0*
- *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*
- *Cisco* Wireless *LAN Controller Command Reference, Release 4.0*

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide*
- *Catalyst 3560 Switch Command Reference*

- *Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*
- *Catalyst 3560 Switch Hardware Installation Guide*
- *Catalyst 3560 Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3560 Switch*

These documents provide complete information about the Catalyst 2960 and 2960-S switches and are available on Cisco.com:

- *Catalyst 2960 and 2960-S Switch Software Configuration Guide*
- *Catalyst 2960 and 2960-S Switch Command Reference*
- *Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*
- *Catalyst 2960-S Switch Hardware Installation Guide*
- *Catalyst 2960-S Switch Getting Started Guide*
- *Catalyst 2960 Switch Hardware Installation Guide*
- *Catalyst 2960 Switch Getting Started Guide*
- *Catalyst 2960 Switch Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, and Spanish
- *Regulatory Compliance and Safety Information for the Catalyst 2960 and 2960-S Switch*

For other information about related products, see these documents:

- *Smart Install Configuration Guide*
- *Auto Smartports Configuration Guide*
- *Cisco EnergyWise Configuration Guide*
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide*
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide*
- For more information about the Network Admission Control (NAC) features, see the *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:
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.
