Release Notes for the Catalyst 3750, 3560, 3560-C, 2960, 2960-S, 2960-C, and 2960-Plus Switches, Cisco IOS Release 15.0(2)SE and Later

October 20, 2014

Cisco IOS Release 15.0(2)SE and later runs on Catalyst 3750, 3560, 3560-C, 2960, 2960-S, 2960-C, and 2960-Plus switches and on Cisco EtherSwitch service modules.

Note Not all Catalyst 3750 and 3560 switches can run this release. These models are *not* supported in Cisco IOS Release 12.2(58)SE1 and later: 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-12S, WS-C3750G-24TS, WS-C3750G-16TD. For ongoing maintenance rebuilds for these models, use Cisco IOS Release 12.2(55)SE and later (SE1, SE2, and so on).

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.

The Catalyst 3560-C switch does not support the IP services image.

These release notes include important information about Cisco IOS Release 15.0(2)SE 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 9.
- 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 9.

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

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

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

Table 1 Catalyst 3750 and Cisco EtherSwitch Service Modules Supported (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
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

Table 2 Catalyst 3560 Switches Supported (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
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, 2960-S and 2960-Plus 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
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

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

Switch	Description	Supported by Minimum Cisco IOS Release
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
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
Catalyst 2960S-F48FPS-L[1]	48 10/100 PoE+ ports (PoE budget of 740 W) and 4 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48LPS-L[1]	48 10/100 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48TS-L[1]	48 10/100 ports and 4 SFP module slots	Cisco IOS Release 15.0(2)SE

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

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960S-F24PS-L[1]	24 10/100 PoE+ ports (PoE budget of 370 W) and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24TS-L[1]	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48TS-S	48 10/100 ports and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24TS-S	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960-Plus 24PC-S	24 10/100BASE-TX PoE ports and 2 dual-purpose ports	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 24LC-S	24 10/100BASE-TX ports (8 of which are PoE) and 2 dual-purpose ports	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 48PST-S	48 10/100B SE-TX PoE ports, 2 10/100/1000 ports, and 2 SFP module slots	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 48TC-L	48 10/100BASE-TX Ethernet ports and 2 dual-purpose ports	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 24TC-S	24 10/100BASE-TX Ethernet ports and 2 dual-purpose ports (no RPS port)	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 48TC-S	48 10/100BASE-TX Ethernet ports and 2 dual-purpose ports (no RPS port)	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 24PC-L	24 10/100BASE-TX PoE ports and 2 dual-purpose ports	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 24TC-L	24 10/100BASE-TX Ethernet ports and 2 dual-purpose ports	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 48PST-L	48 10/100BASE-TX PoE ports, 2 10/100/1000BASE-T copper ports, and 2 SFP module slots	Cisco IOS Release 15.0(2)SE5
Catalyst 2960-Plus 24LC-L	24 10/100BASE-TX ports (8 of which are PoE) and 2 dual-purpose ports	Cisco IOS Release 15.0(2)SE5

1.Support Cisco FlexStack technology.

2.SFP+ = 10 Gigabit fiber uplink.

Table 4 Other Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Cisco CGS 2520 Switch	Cisco 2520 Connected Grid Switch (CGS 2520) is a rugged switch designed for the harsh, rugged environments often found in the energy and utility industries. http://www.cisco.com/en/US/partner/products/ps10978/products_installation_and_configuration_guides_list.html	Cisco IOS Release 12.2(53)EX
SFP modules (Catalyst 3750 and 3560)	1000BASE-CWDM[1], -LX, SX, -T, -ZX 100BASE-FX MMF[2] 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	Cisco IOS Release 12.2(18)SE Cisco IOS Release 12.2(20)SE
SFP modules (Catalyst 2960)	1000BASE-BX, -CWDM, -LX/LH, -SX, -ZX 100BASE-BX, FX, -LX For a complete list of supported SFPs and part numbers, see the compatibility information for SFP modules: http://www.cisco.com/en/US/partner/products/hw/modules/ps5455/products_device_support_tables_list.html	Cisco IOS Release 12.2(25)FX
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 Cisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch) Cisco Redundant Power System 2300	Supported on all software releases Supported on all software releases 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, page 8
- Software Requirements, page 8

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, 7.0, Firefox 1.5, 2.0 or later 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/pcgi-bin/tablebuild.pl/NetworkAssistant

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

Upgrading the Switch Software

- Finding the Software Version and Feature Set, page 9
- Deciding Which Files to Use, page 9

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.150-2.SE.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.150-2.SE.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.150-2.SE.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.
c3560-ipservicesk9-tar.150-2.SE.tar	Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3560c405ex-universalk9npe-tar.150-2.SE .tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager, does not support MACsec encryption.

Table 6 Cisco IOS Software Image Files (continued)

Filename	Description
c3560c405ex-universalk9-tar.150-2.SE.tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager.
c3560c405-universalk9npe-tar.150-2.SE.tar	Catalyst 3560 image with all supported universal image features and Web-based device manager, does not support MACsec encryption.
c3560c405-universalk9-tar.150-2.SE.tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager.
c2960-lanbasek9-tar.150-2.SE.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanlitek9-tar.150-2.SE.tar	Catalyst 2960 LAN Lite cryptographic image file and device manager files.
c2960s-universalk9-tar.150-2.SE.tar	LAN Base and LAN Lite crypto image with device manager
c2960c405ex-universalk9-tar.150-2.SE.tar	Catalyst 2960-C image with all supported universal image features and Web-based device manager.
c2960c405-universalk9-tar.150-2.SE.tar	Catalyst 2960-C image with all supported universal image features and Web-based device manager.
c2960sm-lanbasek9-tar.150-2.SE.tar	Catalyst 2960-SM LAN Base image with Web-based device manager.
c2960-lanbasek9-tar.150-2.EZ.tar	Catalyst 2960-Plus cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanlitek9-tar.150-2.EZ.tar	Catalyst 2960-Plus cryptographic image file and device manager files.

1. SSH = Secure Shell.

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 9 to identify the file that you want to download.

Step 2 Download the software image file:

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

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

b. Navigate to **Switches > 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.

New Software Features

New in Cisco IOS Release 15.0(2)SE5

- Cisco IOS Release 15.0(2)SE5 is now available for Catalyst Switch 2960-Plus.

New in Cisco IOS Release 15.0(2)SE3

- IPv6 Router Advertisement (RA) Guard provides support for allowing the network administrator to block or reject unwanted or rogue RA Guards messages arriving at the network switch platform.

Note This feature is available in the LAN Base feature set.

New in Cisco IOS Release 15.0(2)SE1

- Cisco IOS Release 15.0(2)SE1 on the Catalyst 2960-S, 3750, 3560, 2960-C405, 2960-C405ex, 3560-C405, 3560-C405ex switches has been submitted for certification under FIPS 140-2 and Common Criteria compliance with the US Government, Security Requirements for Network Devices (pp_nd_v1.0), version 1.0, dated 10 December 2010.

  Note The images for the Cisco IOS Release 15.0(2)SE1 on the Catalyst 2960-S, 3750, 3560, 2960-C405, 2960-C405ex, 3560-C405, 3560-C405ex switches are FIPS certified. For information about using FIPS certifies images, see the "Boot Loader Upgrade and Image Verification for the FIPS Mode of Operation" section in the "Assigning the Switch IP Address and Default Gateway" chapter of the software configuration guide.

  FIPS 140-2 is a cryptographic-focused certification, required by many government and enterprise customers, which ensures the compliance of the encryption and decryption operations performed by the switch to the approved FIPS cryptographic strengths and management methods for safeguarding these operations. For more information, see:

  - The security policy document at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1657
  - The installation notes at: http://www.cisco.com/en/US/products/ps10745/prod_installation_guides_list.html

  Common Criteria is an international standard (ISO/IEC 15408) for computer security certification. This standard is a set of requirements, tests, and evaluation methods that ensures that the Target of Evaluation complies with a specific Protection Profile or custom Security Target. For more information, see the security target document at: http://www.niap-ccevs.org/st/vid10488/ .

- Support for Resilient Ethernet Protocol (REP). REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time in ring topologies. See the *Configuring Resilient Ethernet Protocol* chapter in the software configuration guide on cisco.com. (Catalyst 3560-CG and 3560-CPD switches)

New in Cisco IOS Release 15.0(2)SE

- Supports the Universal Power over Ethernet (UPoE) feature. Sources up to 60 W of power (2X 30W) over both signal and spare pairs of the RJ-45 Ethernet cable based on IEEE802.3at standards. Automatically detects UPoE-compliant power devices and negotiates power up to 60 W by using Layer 2 power negotiation protocols, such as CDP or LLDP. It also supplies 60 W power on ports without CDP/LLDP negotiations (for devices that do not support the required UPoE TLV). (Catalyst 2960-C and 3560- C switches)

  For more information on UPoE, see Chapter 15, "Configuring Interface Characteristics" section "Univeral Power over Ethernet" on page 15- 13 of the software configuration guide on Cisco.com.

- Support for IOS IPv6 Host mode, which is compliant with the IPv6 Ready Logo Phase-2 Core Protocols test suite. (LAN Lite image for Catalyst 2960, 2960-C and 2960-S switches; IP Base image for Catalyst 3750, 3750v2, 3560, 3560v2 and 3650-C switches).
- Option to configure a default class on Catalyst 2960-S switches by using the **class class-default** policy-map configuration command. For more information, see the *Configuring QoS* chapter of the software configuration guide on Cisco.com. (Catalyst 2960-S switches)
- Support for OSPFv3 fast convergence. The OSPFv3 link-state advertisements (LSA) and shortest path first (SPF) throttling feature provides a dynamic method to slow down link-state advertisement updates in OSPFv3 during times of network instability. This feature also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds. For more information, see the *Configuring IPv6 Unicast Routing* chapter of the software configuration guide on Cisco.com. (Catalyst 3750 and Catalyst 3560 switches)
- Change in the CLI option relating to OSPFv2 LSA rate limiting. The **all** keyword is now removed from the **timers throttle lsa** global configuration command. (Catalyst 3560-C, 3560v2, and 3750 v2 switches)
- Support for OSPFv3 authentication with IPsec. You can now use the IPsec secure socket API to authenticate OSPF for IPv6 (OSPFv3) packets to ensure that the packets are not altered and resent to the switch. For more information, see the *Configuring IPv6 Unicast Routing* chapter of the software configuration guide on Cisco.com. (Catalyst 3560, 3560-C, 3560v2, 3750, and 3750v2 switches)
- Support for first hop security (FHS) in IPv6. We support the following functions: IPv6 snooping, IPv6 FHS binding, neighbor discovery protocol (NDP) address gleaning, IPv6 data address gleaning, IPv6 dynamic host configuration protocol (DHCP) address gleaning, IPv6 device tracking, neighbor discovery (ND) Inspection, IPv6 port-based access list, IPv6 DHCP guard, IPv6 router advertisement (RA) guard, IPv6 source guard. For more information, see the *Configuring IPv6 Host Functions* chapter of the software configuration guide on Cisco.com. (Catalyst 2960-C, 2960-S and 3560-C switches)
- Support for specifying the VLAN to be used for Smart Install Management. The **vstack startup-vlan** command has been added. For more information, see the command reference on Cisco.com.
- Support for configurable MAC authentication bypass (MAB). You can configure how MAB authentication is performed for client MAC address that deviate from the expected standard format or where the RADIUS configuration requires that the user name and password to differ. For more information, see the *Configuring IEEE 802.1x Port-Based Authentication* chapter in the software configuration guide on Cisco.com.
- Support for negotiating universal PoE (UPoE). For more information, see Updates to the Catalyst 3560 and 2960 Software Configuration Guides, page 67. (Catalyst 2960-C and 3560-C switches)
- Support for Media Access Control Security (MACsec). The switch supports 802.1AE encryption with MACsec Key Agreement (MKA) on downlink and uplink ports for encryption between the switch and host devices. For more information, see the *Configuring MACsec Encryption* chapter in the software configuration guide. (Catalyst 3560-C)
- Support for IKEv2 and IPSecv3 protocols. (IP Base image for Catalyst 3750, 3750v2, 3560, 3560v2 switches)
- Support for Port ACLs on the Layer 2 interface of a switch. (LAN Base image for Catalyst 2960-C and 2960-S switches; IP Base image for Catalyst 3560-C switch)
- Support for Router ACLs on switch virtual interfaces (SVIs). The SVIs may be Layer 3 interfaces to VLANs, physical Layer 3 interfaces, or Layer 3 EtherChannel interfaces. (LAN Base image for Catalyst 2960-C and 2960-S switches; IP Base image for Catalyst 3560-C switch)

- Support for configuring static IPv6 routes in the routing table so that packet data can be sent to networks that are not directly connected to the router. (LAN Base image for Catalys t 2960, 2960-C and 2960-S switches)
- Support for Cisco TrustSec SXP version 2, syslog messages, and SNMP support is now extended to the LAN Base license. (IP Base image for Catalyst 3560-C switch)
- Support for port security on Etherchannels. For more information, see the *Configuring Port-Based Traffic Control* chapter in the software configuration guide.
- Support for IP Source Guard on Etherchannels. For more information, see the *Configuring DHCP and IP Source Guard* chapter in the software configuration guide.
- Support for Precision Time Protocol (PTP) and Temperature and Voltage Monitoring on the Cisco CGS 2520 Switch.

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, 3560, 3560-C, 2960, 2960-S and 2960-C Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Cisco TrustSec SXP version 2, syslog messages, and SNMP support	15.0(2)SE	3560-C, 2960-S, 2960-C
Critical voice VLAN	15.0(1)SE	3750, 3560, 2960-S, 2960
NEAT enhancement to control access to the supplicant port	15.0(1)SE	3750, 3560, 2960-S, 2960
Cisco TrustSec SXP version 2, syslog messages, and SNMP support	15.0(1)SE	3750 and 3560
Auto Smartports improved device classification	15.0(1)SE	3750, 3560, 2960-S, 2960
Device Sensor	15.0(1)SE	3750, 3560
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

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
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

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
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

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
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

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
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

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
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

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
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

Table 7 Catalyst 3750, 3560, 3560-C, 2960, 2960-S and 2960-C 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	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 22
- Device Manager Limitations, page 38

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, page 23
- Ethernet, page 26
- EtherSwitch Modules, page 26
- Fallback Bridging, page 27
- HSRP, page 27
- IP, page 27
- IP Telephony, page 27
- MAC Addressing, page 28
- MAC Addressing, page 28
- Multicasting, page 28

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)

- 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)

- Identity Services Engine (ISE) is not available on Catalyst 2000 series switches.

- The **device-sensor accounting** global configuration command is not available on Catalyst 2000 series switches.

Ethernet

- (Cisco EtherSwitch service modules) 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 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://www.cisco.com/cgi-bin/Support/Bugtool/home.pl

- (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)

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

- When the RSPAN feature is configured on a switch, Cisco Discovery Protocol (CDP) packets received from the RSPAN source ports are tagged with the RSPAN VLAN ID and forwarded to trunk ports carrying the RSPAN VLAN. When this happens a switch that is more than one hop away incorrectly lists the switch that is connected to the RSPAN source port as a CDP neighbor.

  This is a hardware limitation. The workaround is to disable CDP on all interfaces carrying the RSPAN VLAN on the device connected to the switch. (CSCeb32326)

- (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 Cisco EtherSwitch service modules (CSCdy72835):

- (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 Cisco EtherSwitch service modules (CSCdy81521):

- (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 Cisco EtherSwitch service modules (CSCea72326):

- (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, Catalyst 3560 switches, 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)

- 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)

Spanning Tree Protocol

- 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.

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 than if it is on a Gigabit Ethernet 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 master.

Catalyst 2960-S 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.

Cisco IOS Notes

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

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

  If this message appears, 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.

- 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.

- CSCtq35006

  On a switch stack, when an IP phone connected to a member switch has its MAC address authorized using the critical voice VLAN feature, if a master changeover occurs, the voice traffic is dropped. Drop entries for the IP phone appear in the MAC address table management (MATM) table. This occurs because the switch initially drops the voice traffic before reauthenticating critical voice VLAN traffic. The dropped entries are removed when critical voice VLAN authentication occurs.

  There is no workaround. The dropped entries are removed when the IP phone is reauthenticated.

- CSCtr87645

  ASP now uses a device classifier, which determines the type of device that is connected to the switch. As a result, ASP has no control over the protocol type that is used to detect the device. Therefore, the protocol detection controls are deprecated. When you enter the **macro auto global control detection** command, the protocol does not show up in the running configuration; however, the **filter-spec** command is shown in the output.

  There is no workaround. To see the deprecated commands, enter the **show running config deprecated** global and interface configuration command.

- CSCtz87828 (Catalyst 2960-S, 3750, and 3750v2 switches)

  When a cross-stack Etherchannel is used and one of its link is brought down or up, a MAC address learned from this port-channel may either be prematurely cleared from the table or not aged out.

  The workaround is to use a single switch Etherchannel or to clear dynamically-learned MAC addresses after links have been added to or removed from the channel.

- CSCua58659 (Catalyst 2960-S switch)

  The global **power inline consumption default 15400** command fails to restrict the power consumption of a PoE+ port 15.4 W.

  The workaround is to use the **power inline consumption 15400** command in interface configuration mode.

- CSCub20474 (Catalyst 3560, C3560v2, C3750, and C3750v2 switches)

  In a switch stack, multicast traffic can be lost for up to 60 seconds when the master switch is reloaded. Because the platform does not support multicast non-stop-forwarding (NSF), the time before traffic re-convergence after a switchover can vary.

  There is no workaround.

- CSCui89695 (Catalyst Switch 3750)

  When sampled NetFlow is configured with the command **ip flow monitor fm-3 in**, the sampler tables are not exported to the collector.

  The workaround is to use the configuration command **ip flow monitor fm-3 sampler s-1 in**.

- CSCui96470

  While configuring VLAN load balancing using Resilient Ethernet Protocol (REP) on ether channel interface where bundled interfaces are spread across member stack switches, the MAC address flaps when the ether channel state changes from open to alternate.

  There is no workaround.

- CSCuj16899 (Catalyst 2960 and 3750v2 switches)

  System memory may get exhausted on standalone switches with 64 MB of DRAM and stackable switches with 128 MB of DRAM when 802.1x authentication is enabled concurrently with other features. A switch stack of Catalyst 3750v2 switches with more than five members may exhaust system memory and become inoperable.

  The workaround is to limit stacks to five members or fewer.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.0(2)SE7

- CSCef59635

Telnet sessions that are incompletely established may not time out after a period of inactivity, leading to eventual exhaustion of available VTY lines .

When the telnet client initiates a **telnet** session to IOS Server with a small TCP window size (<2) (**rcvwnd** in the client tcp, **sndwnd** in the server side), the target lines are hung for ever. It needs to be manually cleared via **clear tcp** only (clear line does not work). This issue happens for both VTY/TTY sessions.

The workaround is that it needs to be manually cleared via **clear tcp tcb 0xXXXX** only (clear line does not work).

0xXXXX corresponds to hung line.

- CSCsk88751

  The process **Kron CLI Process show tech-support password | redirect tftp..** crashes because of memory corruption. The configuration is as show below:

  kron occurrence Daily-writeNet at 11:50 recurring

  policy-list writeNet

  !

  kron occurrence Daily-showtech at 13:50 recurring

  policy-list showtech

  !

  kron policy-list showtech

  cli show tech-support password \ redirect tftp://194.25.4.197/tech/ms1-ag9!

  kron policy-list writeNet

  cli copy running-config rcp://c@194.25.4.197/ms1-ag9

  !

  The **cli copy running-config rcp://c@194.25.4.197/ms1-ag9** command works, but the **cli show tech-support password | redirect tftp://194.25.4.197/tech/ms1-ag9** command crashes.

  There is no workaround.

- CSCts33952

  When rsh command constructs are used within Tclscript, Tcl fails to send the router hostname which causes the rsh command constructs to fail authorization to a remote router.

  There is no workaround.

- CSCts34693

  An EEM script that executes on a syslog event causes the Cisco router to fail with the following error message.

  *000199: *Aug 23 16:49:32 GMT: %BGP-5-ADJCHANGE: neighbor x.x.x.x Up*

  Exception to IOS Thread:

  Frame pointer 0x30CF1428, PC = 0x148FDF84

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog

  -Traceback=

  1#07279b80de945124c720ef5414c32a90 :10000000+48FDF84 :10000000+48FE400 :10000

  000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FE

F0 :10000000+F5FF94 :10000000+F60608

There is no workaround.

- CSCts87275

  When running the command **show snmp engineID** on a switch with WS-X45-SUP7-E running cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin, it shows same engineID 800000090300000000000000 from different switches. It seems that the switch has picked up interface Fa1 macaddress as its engineID.

  The output is as shown below:

  #show snmp engineID

  Local SNMP engineID: 800000090300000000000000

  #show int f1

  FastEthernet1 is down, line protocol is down

  Hardware is RP management port, address is 0000.0000.0000 (bia 0000.0000.0000)

  The workaround is to manually configure snmp engineID from cli.

- CSCuc90657 (Catalyst 2960s)

  When a 1 gig sfp is inserted in a fuller stack with sierra as master, running the **sh inventory** command does not display the inserted sfp details of the member switch.

  Topology used is stack with sierra as master and fuller as member (both are 48 ports).

  There is no workaround.

- CSCuh03176

  The Privilege commands are not appearing in the configuration of a Catalyst switch.

  When you enter the **privilege interface level 3 switchport port-security mac-address sticky** command and save the configuration, the command is not visible in neither the startup configuration nor the running configuration. However, privilege level 3 users can view the command and can use it. If you reload the switch, the command is still is not visible in the configuration and also becomes unavailable to the privilege level 3 users.

  The workaround is to use the **aaa authorization** global configuration command to access the commands available for a particular user from the AAA server.

- CSCui75238

  A Cisco Catalyst 3750X switch experiences a memory leak when trying use applications like *webauth*, *web_exec* and so on over secure communication (https).

  The workaround is to disable https (secure communication) and use http for HTTP requests.

- CSCum22694

  On the Cisco enhanced EtherSwitch service module (SM-ES2-24P), running the **logging source-interface #** command, does not set the source interface for syslog messages sent to a syslog server.

  There is no workaround.

- CSCum75450

  In a Catalyst 3750X switch stack, the switches experience a slow performance with the following message. Sometimes the switch stops responding and is not recovered until power cycling.

%SUPQ-4-CPUHB_RECV_STARVE: Still seeing receive queue stuck after throttling

You may also observe the following messages when the problem occurs.

%PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism

%XDR-6-XDRIPCNOTIFY: Message not sent to slot X because of IPC error timeout. Disabling linecard. (Expected during linecard OIR)

The issue is observed in switches running 12.2(58)SE or later. It also includes 15.0SE releases and 15.2E releases.

The workaround is to configure a longer logging interval. For example,

ip access-list logging interval <value>

If the issue persists after setting a longer logging interval, you must power cycle the switch.

- CSCum77450 (Catalyst 2960s)

  In a switch stack consisting of Catalyst 2960S switches running 15.0(2)SE4, the MAC address tables on all the stack members are not synchronized with the master switch. This issue is observed when the number of member ports is higher than 4.

  The workaround is to configure the missing MAC addresses manually.

- CSCun01172 (Catalyst 2960s)

  When configuring VLANs on 3750X stacked switches, the CLI experiences a delayed or slow response.

  The workaround is to configure the VTP domain name with VTP enabled.

- CSCun25154

  A change in the behaviour of DHCP client is observed between 15.0(2)SE2 and 15.0(2)SE4 releases.

  There is no workaround.

- CSCun26893

  On a stack of four WS-C3750X-48PF-S switches running IOS "c3750e-universalk9-mz.150-2.SE5.bin", the CPU Utilization is 99%, majorly due to the process "**ASP Process Crea**". The output is as shown:

  b-la1-013-sw-01#sho proc cpu sort

  CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 84%

  --More-- PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process

  PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process

  363 99416 3304 30089 50.39% 43.54% 22.12% 0 ASP Process Crea

  10 843481803 98980536 8521 18.55% 18.03% 18.08% 0 Hulc LED Process

  When trying to remove the macros by running the command "**no macro auto global processing**", the CPU comes back to normal but the master switch crashes.

The workaround is to reload the stack. The CPU remains low for a while. Removing the macros at this time does not cause the master switch to crash.

- CSCun34745

  After system reload, **ip ssh source-interface** shows in startup-config but disappears from running-config. This is seen in both the scenarios as mentioned below.

  <Scenario 1>

1. Configure **ip ssh source-interface <interface>** CLI

   (config)#ip ssh source-interface gi0/3

2. In **show run** output, it will show *ip ssh source-interface <interface>* CLI
3. Configure same <interface> (which is configured in **ip ssh source-interface** CLI) from switch-port to routed-port.

   (config)#interface gi0/3

   (config-if)#no switchport

4. Step 4: In **show run** output, it will not show **ip ssh source-interface <interface>** CLI

   <Scenario 2>

1. Configure some <interface> from switch-port to routed-port.

   (config)#interface gi0/3

   (config-if)#no switchport

2. Configure "ip ssh source-interface <interface>" CLI with same interface mentioned in step 1

   i.e. **(config)#ip ssh source-interface gi0/3**

3. In **show run**" output, it will show "*ip ssh source-interface <interface>*" CLI configured
4. Save the configuration and reload
5. After reload, in **show run** output, it will not show "*ip ssh source-interface <interface>*" CLI

   The workaround is to re-configure **ip ssh source-interface <interface>** CLI.

- CSCun64258

  When around 500 Vlans are configured on a switch running IOS 15.0(2)SE5, and then if the interface is moved down or up, the switch shows high CPU Utilization, with maximum usage by 802.1x switch process for 3 minutes.

  The issue is not seen on switches running IOS 15.0(2)SE4

  The workaround is to disable the device sensor as **no macro auto monitor**.

- CSCun80959

Designated port on the Root Bridge experiences a block forward for 30 seconds. This issue occurs because the message-time (the period of time a packet is alive in the network) is almost equal to max-age (the period of time a packet is allowed to stay in the network). When message-time >= max-age, the switch receives an agedMsg on the forwarding port which moves the port to a blocking state.

There is no workaround.

- CSCun83858

  The lightweight wireless access point macro applied to an interface which has both CDP and LLDP enabled flaps continuously. The CDP neighbor devices are discovered initially on the Gi0 interface of the AP and then after a few seconds, the neighbour devices are discovered on the main interface and the sub-interface (Gi0 and Gi0.1) of the AP. After some time, CDP neighborship times out for the Gi0 interface and the macro configuration for $LINKUP == "NO" event is applied on the switch interface.

  The workaround is to disable LLDP on the switch interface.

- CSCuo17293 (Catalyst 2960s, 2960sf, c2960 and 3750)

  When port-security is configured on all ports and when the end host is moved, the mac address table is out of sync.

  The workaround is to clear the mac address table.

- CSCuo50456 (Catalyst 3560c405ex)

  When port-security is configured on all ports and when the end host is moved, the mac address table is out of sync.

  The workaround is to clear the mac address table.

- CSCuo92394

  When a PC with 802.1x capability is connected to the IP phone, and the PC boots up, the IP Phone sends CDP port UP to the switch, which restarts 802.1x authentication process. The Switch deletes running 802.1x authentication process and starts over upon receiving CDP port UP from the IP phone. It makes authentication process fail on the machines which can only complete it in first run.

  There is no workaround.

- CSCuo97298 (Catalyst 2960)

  On Cisco IOS Release 15.0(2)SE6, the PS-FAN falls to FAUTY status after upgrading the IOS software from Cisco IOS Release 15.0(2)SE5. The **show env stack** command displays the following output:

  SWITCH: 1

  FAN 1 is OK

  FAN 2 is OK

  PS-FAN1 is FAULTY

  PS-FAN2 is NOT PRESENT

  TEMPERATURE is OK

  Temperature Value: 35 Degree Celsius

  Temperature State: GREEN

  Yellow Threshold : 46 Degree Celsius

  Red Threshold : 60 Degree Celsius

POWER is OK

RPS is NOT PRESENT

SWITCH: 2

FAN 1 is OK

FAN 2 is OK

PS-FAN1 is FAULTY

PS-FAN2 is NOT PRESENT

TEMPERATURE is OK

Temperature Value: 34 Degree Celsius

Temperature State: GREEN

Yellow Threshold : 46 Degree Celsius

Red Threshold : 60 Degree Celsius

POWER is OK

RPS is NOT PRESENT

The workaround is to downgrade to Cisco IOS Release 15.0(2)SE5 or to use the latest release which has fix for this issue.

- CSCup49030

  With EX90/EX60 is configured to communicate over the data vlan, EX cannot get ip via DHCP over the data Vlan. This is because switch expects the packet to arrive on voice vlan from EX, but EX is sending packets on data vlan. All DHCP requests get dropped at the switch. Hence EX is not able to get the ip address.

  The workaround is to disable one of the following:

  - Port-security
  - Voice Vlan on the interface (remove voice vlan config from the interface)

- CSCup61889 (Catalyst 2960s, 2960sf, 2960sm and 3750)

  Due to a timing issue, the port channel member port on the slave switch of the stack loops during boot up. The issue occurs only on the member port that is configured as the first port in a cross-stack EtherChannel configuration and when Nexus devices are connected to Cisco devices. Due to Link Aggregation Control Protocol (LACP) graceful convergence, when both the devices are up and in sync (S) state, Cisco devices start transmitting even before the devices get onto collecting (C) state. This causes the port to be pulled down by the Nexus devices. When this happens during boot up, the EtherChannel hardware programming for the port is cleared even when the port is bundled in the port-channel.

  The workaround is to enter the **shutdown/no shutdown** command on the port-channel interface or disable lacp graceful-convergence on the port-channel on peer devices.

- CSCuq06262 (Catalyst 2960s, 2960sf, 2960sm and 3750)

  When a switch stack is configured in VTP client mode with VTP password, the show command for the stack master displays the VTP operating mode as client, whereas the member switches display the VTP operating mode as server.

  The workaround is to remove the VTP password.

- CSCuq49531

10G link convergence is better than 1G convergence during link pull or link down. When the interface is lost in a port channel the flow switch over to the backup link is faster for 10G uplink when compared to a 1G uplink. This is because interface state polling is faster for 10G uplink than 1G uplink.

There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE6

- CSCtl44340 (Catalyst Switches 3750 and 3560)

  On stack switches, the first switch is configured as client and the other switch is configured as DHCP server and TFTP server. When you reload the first switch, the auto configuration does not start.

  There is no workaround.

- CSCto13462 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and c3560C405EX)

  In a network that consists of two DHCP clients with same client id and different mac addresses, the DHCP server reloads when one of the clients releases its DHCP address.

  There is no workaround.

- CSCtr38563 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  Switch fails when a secondary IP address is configured on a VLAN interface.

  There is no workaround.

- CSCts43759 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  The CPU usage increases when you configure the local proxy Address Resolution Protocol (ARP) feature on a Switch Virtual Interface (SVI).

  The workaround is after you configure the SVI, remove the local proxy ARP configuration by entering the **no ip local-proxy-arp** command, and reconfigure it by entering the **ip local-proxy-arp** command.

- CSCts80209 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  A switch configured with login quiet-mode resets when you enter the **login block-for** or **no login block-for** commands.

  There is no workaround. Nevertheless, to avoid a reset, do not enter the **login block** or **no login block-for** commands.

- CSCtz14399 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  The TCP stack of Cisco IOS Software impose a vulnerability caused by terminating the TCP connections incorrectly. This vulnerability can be exploited by allowing an unauthenticated, remote attacker to send a crafted sequence of TCP ACK and FIN packets to an affected device thereby causing an ACK storm which results in excessive network utilization and high CPU usage.

  The workaround is to use the **clear tcp tcb** *0x<tcb_num>*, where the hexadecimal value is the address of the TCB with a connection state of LASTACK in **show tcp brief** command.

- CSCua69378 (Catalyst Switches 3750 and 3560)

When you configure Flex Link on stacks containing interfaces from different switches, the interfaces start flapping continuously.

The workaround is to remove the Flex Link configuration from the interfaces.

- CSCuc63146 (Catalyst Switches 2960, 2960-S, 2960-SM, 3750, and 3560)

  Port-channel interface flaps while adding or removing a VLAN from the trunk on a port-channel interface if one or more port members are not in P or D states.

  The workaround is to shut down the port members which are not in P or D states and make the VLAN changes.

- CSCue95644 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  When you upgrade a device to a Cisco IOS or Cisco IOS XE release that supports Type 4 passwords, enable secret passwords are stored using a Type 4 hash which can be more easily compromised than a Type 5 password.

  The workaround is to configure **enable secret** command on an IOS device without Type 4 support, copy the resulting Type 5 password, and paste it into the appropriate command on the upgraded IOS device.

- CSCue97722 (Catalyst Switches 2960-SF, 2960-S, and 3750)

  In a stack of Catalyst Switches, port security enabled ports block all the network traffic through them. Using the sh mac address-table command shows that the mac address is learned as static on the master switch, whereas the member switches do not have this mac address on their mac address table.

  There is no workaround.

- CSCug42311 (Catalyst Switch 2960-S)

  Configuring **logging buffered** *[size]* command with large buffer size causes the switch to experience an out of memory or low memory condition.

  The workaround is to reduce the logging buffer allocation using the CLI.

- CSCug47095 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960c405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  During the SNMP walk, the **vlanTrunkPortDynamicStatus** object in the CISCO-VTP-MIB module shows " notTrunking(2)” for the members of Port-channel trunk ports.

  The workaround is to use the CLI to get the correct values.

- CSCug52922 (Catalyst Switches 2960, 3560, and 3750)

  The DHCP Snooping or the IP Device Tracking (IPDT) feature does not work when you upgrade the switch to Cisco IOS release 15.0(2) SE5. The host IP address is not displayed when you run the **sh auth sess int det** command.

  There is no workaround.

- CSCug90127 (Catalyst Switches 2960-S, 2960-SM, and 3750)

  The switch port goes in to the err-disabled state due to port security violations.

  The workaround is to run the **no switchport** command on the interface.

- CSCuh45966 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

Device under test (DUT) fails with traceback when you enter the **configure replace** *target-url* command. The issue occurs when the following message is forwarded to forward_formatted_msg_to_logger() API.

```
% eula should be accepted for non-interactive management for license-level =
ipservices (stack3-1-3I-1-2)
```

There is no workaround.

- CSCuh72558 (Catalyst Switches 2960-S, 2960-SM, 2960-SF, and 3750)

  In a switch stack, if a stack member is connected to a Meru access point that requires 802.3at or 29.5W POE+ inline power, the connection over 802.3at POE+ fails.

  The workaround is to move all the affected POE+ devices to the stack master.

- CSCuh91853 (Catalyst Switch 3560CX)

  When the switch is run on the IPBase license and when you enter the **show sdm prefer** command, the IPV6 entries are not displayed though the IPV6 feature is supported.

  There is no workaround.

- CSCui07884 (Catalyst Switches 2960-S and 3750)

  The stacked switch setup fails when you change or remove an existing password while the relayed console waits for the authentication prompt.

  The workaround is to reduce the number of changes to the password in the console or VTY when the relayed console waits for the authentication prompt.

- CSCui20519 (Catalyst Switch 2960-S)

  In a Cisco Catalyst Switch stack of 8 member switches, a memory leak is observed in the HRPC pm request handler process. The issue occurs after reloading the stack members or after online insertion and removal (OIR) of the transceivers that are DOM capable.

  There is no workaround.

- CSCui52743 (Catalyst Switches 3750 and 3560)

  When you enable the Address Resolution Protocol (ARP) retry feature on the switch, the CPU usage increases.

  There is no workaround.

- CSCui56736 (Catalyst Switches 2960-S and 3750)

  When VLAN Trunk Protocol (VTP) version 3 is configured on stacked switches, the inconsistency in VTP mode is observed between the master switch and the member switch. When you run the **show vtp status** command, the master switch shows the status as Server for VLAN and Transparent for Multiple Spanning Tree (MST), and the member switch shows the status as Primary Server for both VLAN and MST.

  The workaround is to configure the switch to VTP version 2 and then reconfigure the switch to VTP version 3.

- CSCui59769 (Catalyst Switch 3750)

  The Web Cache Communication Protocol (WCCP) traffic drops when you reload the master switch with the stack switch.

  There is no workaround.

- CSCuj36089 (Catalyst Switches 3750 and 3560)

In a topology in which a Catalyst 3750X switch acts as the multicast router, a receiver constantly sends join messages to a multicast group (*,G) before the source starts sending the multicast traffic. When the source starts sending traffic to the multicast group, an (S,G) is created and some of the initial packets sent by the source are lost. Once the (S,G) is programmed for the traffic sent by the source, all the subsequent multicast traffic reaches the receiver.

There is no workaround.

- CSCuj48700 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  A switch reboots unexpectedly while using dot1x authentication with IP Device Tracking (IPDT) enabled. If **ip device tracking probe** {**delay** *delay*} is configured and the switch is operating near the maximum IPDT limit of 2048 hosts, there is a probability that a host may have its delay timer started, but released before it expires.

  Use one of the following workarounds:

  - Keep the number of hosts less than 2048.
  - Turn off probe delay.
  - Disable dot1x authentication, which in turn disables IP HOST TRACK process.

- CSCuj54648 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960-LM, 3750, 3560, and 3560C405)

  The blocked port on a Catalyst Switch, receives and forwards a malformed TCP packet thereby causing the packet to loop continuously in the network and flooding to all the ports of the VLAN.

  Use one of the following workarounds:

  - Enter the **shut** or **no shut** command on any of the ports in the topology.
  - Change the Spanning Tree Protocol (STP) priority of any of the switches in the topology.
  - Downgrade the switch to 12.2(35)SE5 and the malformed TCP packet is dropped on the blocked port.

  CSCuj65057 (Catalyst Switches 2960-SF, 2960-S, and 3750)

  When you configure per-VRF on a AAA TACACS+ server group, the **ip vrf forwarding** command does not appear in the running configuration after reloading the stack master. This issue takes place only in stack configurations.

  The workaround is to use **vrf definition** command instead of **ip vrf** command to configure per-VRF.

- CSCuj77254 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  Access Control List (ACL) configured on guest VLAN interface for 802.1X unauthenticated clients do not get applied.

  The workaround is to configure the ACL on the dot1x port itself instead of the guest VLAN interface.

- CSCuj77426 (Catalyst Switches 2960, 2960-S, and 3560)

  After performing a **shut** or **no shut** on the ports of a Catalyst Switch, the status of some of the ports are displayed as **Not Connected**, even if they are connected to a remote device.

  The workaround is to perform a **shut** or **no shut** on the affected ports.

- CSCul00921 (Catalyst Switch 2960-P)

  In the switch running earlier to Cisco IOS software release 12.2(52)SE, the switch displays “Error loading flash” messages when restarted.

The workaround is to upgrade the switch to Cisco IOS software release 12.2(52)SE or later.

- CSCul02715 (Catalyst Switches 3750, 3560, 3560C405, 3560C405EX)

  The switch reboots if the **shutdown** and **no shutdown** commands are repeatedly entered for the alternating ports in an 8-node Resilient Ethernet Protocol (REP) ring segment. The following error message is displayed:

  ```
  Debug Exception (Could be NULL pointer dereference) Exception (0x2000)
  ```

  There is no workaround.

- CSCul17159 (Catalyst Switches 2960, 2960-LANLITE, 2960-SF, 2960C405, 2960C405EX, 2960-LM, 2960-S, 2960-SM, 3750, 3560, 3560C405, and 3560C405EX)

  In response to an NTP control request, the offset value in the reply packet received from a Catalyst 3560X/E switch running on 12.2(58)SE or later is different from the offset value in a packet received from a switch running on 12.2(55)SE or earlier.

  The workaround is to downgrade the switch to 12.2(55)SE or earlier.

- CSCul17852 (Catalyst Switches 3750, 3560, 3560C405, and 3560C405EX)

  When you repeatedly run the **shut** and **no shut** command in the alternating ports on a 8 node REP ring, the stack member with REP secondary edge port drops the multicast traffic for 20 to 50 seconds.

  There is no workaround.

- CSCum78626 (Catalyst Switches 2960-S, 2960-SF, 2960-SM and 3750)

  When a new switch is added to the stack, and if the stack has the Hot Standby Router Protocol (HSRP) configured, the newly added member switch fails.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE5

- CSCty66702 (Catalyst Switch 3750)

  In Policy Based Routing (PBR), if the first match clause is removed, the packets are forwarded to the next hop IP address of the second match clause. This feature, which previously showed errors, is now functioning properly.

  There is no workaround needed.

- CSCua74302 (Catalyst Switches 2960 and 2960-C)

  (LAN Base) ACLs applied to outbound traffic on the switch virtual interface (SVI) do not work.

  There is no workaround.

- CSCud17658 (Catalyst Switch 2960-S)

  If a 100BaseFX-SFP module is used in the switch, data packets on this interface may drop over this link.

  The workaround is to reinsert the module into the switch.

- CSCud47137 (Catalyst Switch 2960-S)

  After a master switch failure, the member link within an LACP-enabled EtherChannel fails to recover.

  The workaround is to enter the **shutdown** command followed by the **no shutdown** command, which will recover the failed links.

- CSCud86438 (Catalyst Switch 3750-G)

  The "HULC DOT1X Process" leaks memory on the switch stack member. Sometimes the following `log message is displayed:`

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to insufficient processor memory
  ```

  There is no workaround.

- CSCuf82297 (Catalyst Switch 3560-C)

  The command power inline port 2x-mode was not supported on the switch. This has now been fixed.

  There is no workaround.

- CSCug14754 (Catalyst Switch 2960-SF)

  Cyclic Redundancy Check (CRC) errors appear on switch with Fast Ethernet module operating at 10 Mb half-duplex mode.

  There is no workaround.

- CSCug26848

  CPU usage goes above 90% when Internet Group Management Protocol (IGMP) version 3 report packets are sent to the switch which has IGMP version 2 configured on the switch virtual interface.

  The workaround is to either disable multicast fast convergence or configure IGMP version 3 on switch virtual interface.

- CSCug52714

  TACACS+ single connect authentication request from a switch stack takes around 10 to 12 minutes to failover to secondary server after the primary TACACS server is unreachable.

  The workaround is to disable TACACS+ single connect configuration on the switch.

- CSCui41032

  Switch runs out of memory within few seconds of configuring the **level <n> show spanning-tree active/detail** privilege EXEC command.

  There is no workaround.

- CSCui73360 (Catalyst Switch 2960)

  Switches that run Cisco IOS Release 15.0(02.01.12)SE4 do not support 8k MAC addresses with IPv6 templates.

  There is no workaround. 8k MAC address are supported on the dual-ipv4-and-ipv6 VLAN template introduced in Cisco IOS release 15.0(02.01.12)SE05.

- CSCui87793

  Web authentication does not work.

  There is no workaround.

- CSCui90464 (Catalyst Switch 3560-C)

  MACsec link traffic drops periodically.

  There is no workaround.

- CSCuj81084

  In a switch stack where EnergyWise is enabled, memory leak is observed when the **show energy wise children** privileged EXEC command is entered or when the `cewEntEnergyUsage` object ID is polled.

The workaround is to disable EnergyWise.

Caveats Resolved in Cisco IOS Release 15.0(2)SE4

- CSCug62154

  When the switch is started using TACACS+ configurations, the CPU utilization increases to 100% and the VTY device does not work.

  The workaround is to remove the TACACS+ configurations and restart the switch.

- CSCuh41077

  The ipAddrEntry value in the IP Address Table shows an interface index that is not exposed by the ifEntry Object ID.

  There is no workaround.

- CSCuf77683

  Internal VLANs are displayed when the **show snmp mib ifmib ifindex** command is entered or the SNMP is queried for the ipMIB object.

  The workaround is to check if the displayed VLANs are internal and then to hide them.

Caveats Resolved in Cisco IOS Release 15.0(2)SE3

- CSCta43825

  CPU usage is high when an SNMP Walk of the Address Resolution Protocol (ARP) table is performed.

  The workaround is to implement SNMP view using the following commands:

  snmp-server view cutdown iso included

  snmp-server view cutdown at excluded

  snmp-server view cutdown ip.22 excluded

  snmp-server community public view cutdown ro

  snmp-server community private view cutdown rw

- CSCts95370

  If an ACL is configured on a router VTY line for ingress traffic, the ACL is applied for egress traffic also. As a result, egress traffic to another router on an SSH connection is blocked.

  The workaround is to permit egress traffic to the specific destination router using the **permit tcp host** <*destination router IP address*> **eq 0 any** interface configuration command.

- CSCub45763

  The device connected to the switch crashes when a CDP data frame is processed. The `SYS-2-FREEFREE` and `SYS-6-MTRACE` messages are displayed.

  The workaround is to disable CDP using the **no cdp run** global configuration command. This workaround is not applicable if the connected device relies on or supports a phone or voice network.

- CSCub54295 (Catalyst 3560 and 3750 switches)

The service module fails when the TestPortAsicRingLoopback online diagnostic test is run.

There is no workaround.

- CSCub85948

  Memory leak is seen in the switch when it sends CDP, LLDP or DHCP traffic and when the link flaps.

  The workaround is to apply protocol filters to the device sensor output by entering the following global configuration commands:

  no macro auto monitor

  device-sensor filter-spec dhcp exclude all

  device-sensor filter-spec lldp exclude all

  device-sensor filter-spec cdp exclude all

  If the memory leak continues in the "DHCPD Receive" process, disable the built-in DHCP server by entering the **no service dhcp** global configuration command.

- CSCuc10143 (Catalyst 3750, 3560, 2960, 2960-S, 2960-SF, and 2960-SM switches)

  Spurious traps observed periodically on removal of power to RPS.

  There is no workaround.

- CSCuc40634

  STP loop occurs on Flexstack connected by parallel links when a link state is changed on Flexlink port.

  The workaround is to change the switch to root bridge.

- CSCuc41395 (Catalyst 3750 and 3560 switches)

  Policy Based Routing (PBR) entry on the switch does not become inactive even after the PBR route's next hop is lost. The traffic continues to take failed PBR path instead of the next available best path.

  There is no workaround.

- CSCud19122 (Catalyst 2960, 2960-C, 2960-SF, 2960-S, and 2960-SM switches)

  Duplex status configured on 100BASE-FX SFP interface changes from full to half when shut/no shut command is run on the interface.

  The workaround is to delete the duplex full configuration and configure again.

- CSCud44884

  If a policy map attached to the switch interface is modified then the corresponding QoS policy works incorrectly.

  The workaround is to delete the policy map, create a new policy map and then attach it to the interface.

- CSCud76611 (Catalyst 3750 and 3560 switches)

  The switch blackholes traffic redirected by Web Cache Communication Protocol (WCCP). This issue occurs when the WCCP cache engine is shut down and the cache is not cleared.

  The workaround is to use Cisco IOS Release 12.2(55) or later.

- CSCud83248

  When native VLAN is configured on the trunk or when switchport trunk native vlan 99 is configured on the interface, spanning-tree instance is not created for native VLAN.

The workaround is to keep VLAN1 as a native on the trunk. In Cisco IOS Release15.0(2) SE, **dot1.x** is enabled by default and causes authentication fail in the native VLAN. This results in **pm_vp_statemachine** not triggering any event to spanning tree. To disable **dot1x** internally, run the **no macro auto monitor** command. The stp instance is created for native vlan 99 after running the **show** and **no show** command on the interface.

- CSCue03558 (Catalyst 3750 switch)

  When a member of 3750 stack is reloaded, the uplink trunk connected to Catalyst 4500 switch becomes non-trunk causing STP issues on the switch. The STP reports the stack port as root port instead of Gi2/0/1.

  When a member of 3750 stack with fiber SFP uplinks is reloaded, it results in STP issues on the stack and the internal stack ports on the switch becomes the root port.

- CSCue27509 (Catalyst 2960 and 3560 switches)

  CRC errors are reportedwhen traffic is sent from the peer ports of a switch.

  There is no workaround.

- CSCue34250 (Catalyst 3560 and 3750 switches)

  The Web Cache Communication Protocol (WCCP) traffics are not redirected after reloading the switch.

  The workaround is to remove the WCCP redirects command from the interface and then add them back on the interface.

- CSCue54767 (Catalyst 2960, 2960-G, 3750, 3750-G, 3560, and 3560-G switches)

  TCP fragmented packets cannot be sent for SPAN monitor session.

  The work around is to use the egress span iso of the ingress span and span the malformed TCP packets to span destination port as there are no classification checks in the egress interface for parse fail conditions.

- CSCue86180

  On the Catalyst 2960S switch stack, when the login block command is configured and the running config is saved using the **wr** command on the master, it brings the master down. When the running config is saved on the new master , the following lines are displayed on entering the show running-config command.

  ip access-list extended sl_def_acl

  deny tcp any any eq telnet

  deny tcp any any eq www

  deny tcp any any eq 22

  permit ip any any

  There is no workaround.

- CSCue87815

  When the secret password is configured, the password is not saved. The default password is used as the secret password.

  The workaround is to use the default password to login and then change the password.

- CSCue92705

The device sensor related memory leak is still visible in DHCPD Receive, CDP Protocol, and Net Background processes even after disabling the device sensor feature by entering the no macro auto monitor command. This symptom is observed in Cisco IOS 15.0(2)SE1 Release, 2960-S, dhcp, cdp traffic, and link flapping.

The known workaround is to enter the no service dhcp command if the switch is not a DHCP server and configure the device sensor as follows:

device-sensor filter-spec cdp exclude all

device-sensor filter-spec dhcp exclude all

device-sensor filter-spec lldp exclude all

Caveats Resolved in Cisco IOS Release 15.0(2)SE2

- CSCtg15739

  When a client fails to authenticate in the multi-auth mode, the session continues to be active indefinitely.

  The workaround is to enter the **clear authentication sessions** privileged EXEC command to clear information for all authentication manager sessions.

- CSCty63718

  The **down-when-looped** interface configuration command is not supported with default speed or with 1000BaseT advertisements on the gigabit medium independent interface (GMII interface). This is because the down-when-looped feature and 1000BaseT advertisements both make use of the "next page" function as defined in IEEE 802.3, clause 28 and may result in the link staying down.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE1

- CSCee32792

  When using SNMP v3, the switch unexpectedly reloads when it encounters the snmp_free_variable_element.

  There is no workaround.

- CSCtg39957

  The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

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

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp

Note The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

Note The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCth03648

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

  The workaround is to disable all SNMP traps.

- CSCth59458

  If a redundant power supply (RSP) switchover occurs during a bulk configuration synchronization, some of the line configurations might disappear.

  The workaround is to reapply the line configurations.

- CSCti95154 (Catalyst 2960, 2960-S, 3560, and 3750 switches)

  Beginning with Cisco IOS Release 12.2(52)SE, the device tracking table could map only one IP address to a single MAC address. This restriction has been removed, and several IP addresses can now be mapped to a single MAC address.

- CSCtl12389

  The **show ip dhcp pool** command displays a large number of leased addresses.

The workaround is to turn off **ip dhcp remember** and reload the switch.

- CSCtq64716

  The following warning messages might be displayed during the boot process even when a RADIUS or a TACACS server have been defined:

  ```
  %RADIUS-4-NOSERVNAME:
  ```

  or

  ```
  %AAAA-4-NOSERVER: Warning: Server TACACS2 is not defined
  ```

  There is no workaround.

- CSCtq75383 (Catalyst 2960 switches running the Cisco IOS LANLite images)

  The **traceroute** command returns the error message:

  ```
  % VRF  is not accessible.
  ```

  There is no workaround.

- CSCtr37757

  The secure copy feature (**copy:** *source-filename* **scp**: *destination-filename* command) does not work.

  There is no workaround.

- CSCtw33903

  This problem occurs when the Enterprise Policy Manager (EPM) for a device connected to an interface is authorized in closed mode and no policies are configured or downloaded. If no port ACL is configured, the auth-default access control list (ACL) is applied to the switch. If another device is connected to this device, restricted VLAN (**authentication event** interface configuration command) is enabled on the port. The Application Control Engine (ACE) is not configured to permit traffic originating from the connected device, and IP packets are dropped.

  The workaround is to configure a port ACL to allow IP traffic for the specific IP range for the connected devices on the interface.

- CSCtw89960 (Catalyst 3560-C switch)

  When Catalyst 3750 switch or Catalyst 3560 is configured as a Layer 3 switch with local connected hosts, the switches drop large IPv6 traffic loads intended for local connected hosts.

  The workaround is not to globally configure IPv4 VRF.

- CSCtx69656 (Catalyst 3560-C, 2960-C, and 2960-S switches)

  If a Catalyst 2960 switch boots with Cisco IOS Release 12.2(50)SE5 or later, a Catalyst 3750 switch that is connected by a trunk port to the Catalyst 2960 switch cannot receive the Generic Attribution Registration Protocol (GARP) data packets from the Catalyst 2960 switch.

  The workaround is to perform the following actions:

  - Run the Catalyst 2960 switch on Cisco IOS Release 12.2(25)SEE or 12.2(53)SE2.

  - Clear the Address Resolution Protocol (ARP) on the connected device.

  - Enter the **switchport noneg** command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent to the Layer 2 interface.

  - Ping from the Catalyst 2960 switch to the connected device.

  - Use the **line-proto-delay** command to control Switch Virtual Interface (SVI) timing.

- CSCty10239

  When ipl=5, the Catalyst 2960 switch receives the malloc failure message of 20 bytes, and traceback occurs due to interrupt level.

  There is no known workaround.

- CSCty81591 (Catalyst 2960-S switch)

  A Platform assert failure message is displayed on the switch. Traceback occurs after deleting the static mac-address table

  The workaround is to set the dynamic mac-address table and to ensure that the return value of the API that allocates SD is checked correctly.

- CSCtz13824 (Catalyst 3750-G, 3560-G, and 2960-G switches)

  Customers unable to appy Quality of Service (QoS) policy-map on interface on more than 4 ports on different ASIC on a switch. This issue is common to Catalyst 2960G, 3560G, and 3750G switches having more than one ASIC.

  There is no known workaround.

- CSCtz91389 (Catalyst 3750-G, 3560-G, and 3750-V2, 3560-V2 switches)

  When the **ip rsvp snooping** command is enabled on a Layer 2 environment, the switch stops forwarding the metadata packets.

  There is no known workaround.

- CSCtz96168 (Catalyst 3750-G, 3560-G, and 3750-V2, 3560-V2 switches)

  IPv6 packets are forwarded between two isolated ports in the same private VLAN.

  There is no known workaround.

- CSCtz98066 (Catalyst 2960-S switch)

  When the master switch (Switch A) is reloaded or loses power and rejoins the stack as a member switch, any traffic stream that exits Switch A is dropped because the newly joined member is not able to establish an Address Resolution Protocol (ARP) entry for the next hop router or switch. Debugs confirm that Switch A does not send a GARP or ARP for the next hop, though traffic continues to be sent to the switch.

  The workaround is to add a static ARP. Ping the destination from Switch A to force the ARP to respond.

- CSCtz99447

  Local web authorization and HTTP services on the switch do not respond because of a web authorization resource limitation in the system. The resource limitation is normally caused by incorrectly terminated HTTP or TCP sessions.

  These are possible workarounds and are not guaranteed to solve the problem:

  - Enter the **ip admission max-login-attempts** privileged EXEC command to increase the number of maximum login attempts allowed per user.
  - If the web authorization module is intercepting HTTP sessions from web clients in an attempt to authorize them, try using a different browser.
  - Eliminate background processes that use HTTP transport.

- CSCua64859

  The CISCO_LAST_RESORT_AUTO_SMARTPORT macro is applied to any device for which there is no built-in or user-defined macro, regardless of whether the device supports CDP, Link Layer Discovery Protocol (LLDP), or DHCP. To ensure that a device is not running a discovery protocol that matches the device to a built-in or user-defined macro, the switch waits about 120 seconds before applying the CISCO_LAST_RESORT_AUTO_SMARTPORT macro. The macro is applied to devices such as PCs, laptops, and printers. You do not need to configure MAC operationally unique identifier (OUI)-based triggers and map these triggers to a macro for these devices.

- CSCub55790

  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

  Affected devices that are configured as Smart Install clients are vulnerable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall

- CSCub93357

  If an interface is configured with the **switchport port-security maximum 1 vlan** command, the following error message is displayed:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
  address XXXX.XXXX.XXXX on port <interface>
  ```

  There is no workaround.

- CSCuc03555

  The flash memory is corrupted when you format the flash manually.

  The workaround is to reload the switch. (Note that this will erase the flash memory, and you will need to reload the software image using TFTP, a USB drive, or a serial cable.

- CSCuc04407 (Catalyst 3560 switch)

  VLAN-based QoS is not available on interfaces on the WS-C3560CG switches.

  There is no workaround.

- CSCuc17720

  If the Performance Monitor cache is displayed (using the **show performance monitor cache** command) and you attempt to stop the command output display by entering the **q** keyword, there is an unusually long delay before the output is stopped.

  The workaround is to enter the **term len 0** privileged EXEC command so that all command outputs are displayed without any breaks.

- CSCuc36990 (Catalyst 3560 switch)

  Cisco TrustSec Media Access Control Security (MACsec) cannot be configured on uplink ports. MACsec interface commands are not accepted on the switch except when you enter the **sap pmk** *key* **modelist no-encap** command. This issue is seen on switch model WS-C3560CG for interface range GigabitEthernet0/9 to GigabitEthernet0/10.

  The workaround is to configure Cisco TrustSec MACsec the on RJ45 Gigabit Ethernet ports for interface range GigabitEthernet0/1 to GigabitEthernet0/8. There is no workaround for Cisco TrustSec MACsec configuration on Gigabit Ethernet optical links.

- CSCuc53848 (Catalyst 3560 switch)

  The **device-sensor accounting** global configuration command is not available.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE

- CSCtk12589 (Catalyst 2960-S switch)

  When a Catalyst 2960S series switch is booted up, a large number of Yeti2S88gMdioWr: Unknown status for write operation messages may be written to the console. Although the error messages may substantially increase bootup time, the switch is fully functional after Cisco IOS boots.

  The workaround is to power cycle the switch for a quick recovery. This is a software issue and the switch does not require replacement.

- CSCtl41917 (Catalyst 2960-S switch)

  When a switchover occurs in a switch stack, the host session information is lost.

  The workaround is to reauthenticate all the clients.

- CSCtl48226

  When the **show epm session summary** or **show epm** command is entered from an SSH or telnet session and another command is entered from the console, the switch might unexpectedly reset and generate crash information.

  The workaround is to enter both commands from the same session, either SSH/telnet or console.

- CSCtl60151

  The switch might occasionally reload after experiencing a CPU overload, regardless of what process is overloading the CPU.

  There is no workaround.

- CSCto09117

  The switch downloads the running IOS image from the TFTP server and reboots even though the same image is currently loaded and running.

  There is no workaround.

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

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

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCtq38500 (Catalyst 2960-S switch)

  When an interface is configured with the **mls qos** command, traffic is not matched by port-based QoS ACLs that use the range option.

  The workaround is to is to configure the switch using the single port eq keyword. Alternatively, you can configure the trust under class-default setting for the same policy-map that uses the acl-range option.

- CSCtq51049 (Catalyst 2960-S, 2960SM, 3750, and 3750v2 switches)

  In a switch stack, you cannot establish a console session with a member switch when an ACL is applied to the VTY lines.

  The workaround is to use the following procedure when you apply an ACL to line vty 0 4 and line vty 5 15:

  1. Create the **vty** ACL and permit the 127 network.
  2. Append the **vrf-also** keyword to the configured access-class inbound.

  See the following example:

```
ip access-list standard vty-acl
   permit 127.0.0.0 0.0.0.255

line vty 0 4
   access-class vty-acl in vrf-also
   privilege level 15
   length 0
   transport input ssh
line vty 5 15
   access-class vty-acl in vrf-also
   privilege level 15
```

```
transport input ssh
```

- CSCtq86186 (Catalyst 2960-S)

  In a switch stack, the **show interface** command shows incorrect values for output drops.

  The workaround is to use the **show platform port-asic stats drops** command to see the correct values.

- CSCtr07908

  The archive download feature does not work if the flash contains an “update” directory. This situation is likely to occur if a previous download failed or was interrupted and the “update”” directory is still left in the flash.

  The workaround is to delete the “update” directory in the flash before starting the archive download.

- CSCtr19734 (Catalyst 2960-S, 3750, and 3759v2 switches)

  A static route that has the next hop set to null0 is removed when the master switch is changed in a switch stack configuration. This situation occurs when the switch is stacked and the static route is advertised by the **network 0.0.0.0** command.

  The workaround is to use the **ip summary-address eigrp** *as-number ip-address mask* command to set the IP summary aggregate address for the interface through which the next hop can be found.

- CSCty88456

  The Catalyst 4500E series switch with Supervisor Engine 7L-E contains a denial of service (DoS) vulnerability when processing specially crafted packets that can cause a reload of the device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ecc

- CSCtr32202 (Catalyst 2960-S switch)

  When ports from each switch in a switch stack are bundled together to form an uplink port channel, Multicast VLAN Registration (MVR) streams are sent only to the switch with the active member in the port channel.

  The workaround is to use Internet Group Management Protocol (IGMP) snooping.

- CSCtr44361 (Catalyst 2960-S, 3750, and 3750v2 switches)

  When a device is moved from one port to another in a switch stack, the SNMP data generated for the move event is incorrect.

  The workaround is to ensure that the uplink to the core network is configured on the master switch (for example, a 1/0/x port).

- CSCtr55645

  OSPFv3 neighbors might flap because of the way the switch handles IPv6 traffic destined for well-known IPv6 multicast addresses.

  There is no workaround.

- CSCts36715

  Users connecting to the network through a device configured for web proxy authentication may experience a web authentication failure.

  There is no workaround. Use the **clear tcp tcb** command to release the HTTP Proxy Server process.

- CSCtt11621

  Using the **dot1x default** command on a port disables access control on the port and resets the values of the **authentication host-mode** and **authentication timer reauthenticate** commands to the default values.

  The workaround is to avoid using the **dot1x default** command and set various dot1x parameters individually. You can also reconfigure the parameters that were changed after you entered the **dot1x default** command.

- CSCtt19547 (Catalyst 3560, 3560v2, 3750, and C3750v2)

  The switch drops Layer 3 multicast traffic received from a Layer 2 port channel on a switch virtual interface (SVI) that is associated with a VPN Routing and Forwarding (VRF) instance.

  The workaround is to flap the ingress physical interface, the SVI, or the port channel.

- CSCtt98094 (Catalyst 2960-S switch)

  In a switch stack setup after you reload a member switch, a multilayer switching (MLS) class of service (CoS) configuration command with a specified value such as **mls qos cos 7** on the slave switch does not function anymore. This situation impacts untagged IP and Layer 2 packets.

  The workaround is to ensure that when you configure a service policy on an interface, an interface default level CoS is also configured. You can use **mls trust qos cos** command in interface configuration mode.

- CSCtw98934 (Catalyst 2960-C and 2960-S switches)

  Frame check sequence (FCS) errors occur when the switch receives jumbo frames (greater than 9000 bytes) on downlink ports.

  There is no workaround.

- CSCtx33436

  When using the **switchport port-security maximum** 1 **vlan access** command, if an IP-phone with a personal computer connected to it is connected to an access port with port security, a security violation will occur on the interface. This type of message is displayed on the console:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
  XXXX.XXXX.XXXX on port FastEthernet0/1.
  ```

  Here is a sample configuration:

  ```
  interface gigabitethernet 3/0/47
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 3
  switchport port-security maximum 2
  switchport port-security maximum 1 vlan access
  switchport port-security maximum 1 vlan voice
  switchport port-security
  ```

  The workaround is to remove the line **switchport port-security maximum** 1 **vlan access**.

- CSCtx96491

  The switch does not correctly detect a loopback when the switch port on an authenticated IP phone is looped to a port configured and authenticated with dot1x security, even when **bpduguard** is configured on the interface. This situation can result in 100 percent CPU utilization and degraded switch performance.

  The workaround is to configure the interface with the **authentication open** command or to configure **authentication mac-move permit** on the switch.

- CSCue23882 (Catalyst Switches 3750 and 2960-S)

  If a new port is added to an etherchannel on a switch using DAI or IPDT, ARP packets that ingress the port are lost.

  The workaround is to save the configuration and reload the switch. Alternatively, configure the switch by entering the **no macro auto monitor** command followed by the **macro auto monitor** command after the port is bundled for the first time.

- CSCuj16899 (Catalyst 2960 and 3750v2 switches)

  The system memory on some switches (standalone switches with 64MB of DRAM, and stackable switches of more than 5 members with 128MB of DRAM each) may be exhausted when 802.1x authentication is enabled concurrently with other features.

  The workaround for 3750v2 stacks is to limit the setup to 5 switches. If more then 5 switches are required in a stack, keep the number of VLANs and enabled features as low as possible. The workaround for 2960 switches with 64MB of DRAM is to maintain 1MB of memory free all the time.

Documentation Updates

Updates to the Catalyst 3560 and 2960 Software Configuration Guides

Information Added to the "Configuring Interface Characteristics" Chapter

In the "Configuring Interface Characteristics" chapter, this new section was added:

Universal Power over Ethernet Support

Cisco Universal Power over Ethernet (UPoE) is a Cisco proprietary technology that extends the IEEE 802.3 PoE standard to provide up to 60W of power over standard Ethernet cabling infrastructure (Class E or better). UPoE power negotiation uses Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP), to which proprietary type-length-value (TLV) elements have been introduced. UPoE is available only when both the powered device (PD) and the power sourcing equipment (PSE) support these additional TLVs.

The Catalyst 2960-C and 3560-C switches have both PD and PSE capabilities. These switches support UPoE on one uplink interface at a time and negotiate power of up to 60 W from a parent PSE. On the downlink interfaces, the switches are capable of sourcing IEEE 802.3af PoE only.

Guidelines and Limitations

- Because CDP is enabled on the switch by default, no special configuration is required to enable UPoE negotiation. If you want to used LLDP instead of CDP, disable CDP and enable LLP in global configuration mode, followed by the **shutdown/no shutdown** command sequence on the interface of parent switch.

- In general, the switch cannot negotiate UPoE power when both uplinks are connected to a PoE-capable PSE. The exceptions are when one of the uplinks is connected to a data-only interface on the PSE or when the first uplink has negotiated UPoE power. When the first uplink negotiates UPoE power, the second uplink behaves like a data-only interface.
- Table 8 shows the valid configurations when the switch is connected to a UPoE-capable PSE.

Table 8 Catalyst 2960-C and 3560-C Switch Connected to UPoE-Capable PSE

Powered Device Uplink 1	Powered Device Uplink 2
UPOE	Data only
Data only	UPOE

- Table 9 shows the amount of power available for pass-through PoE when the switch has negotiated UPoE.

Table 9 Power Available for Pass-through PoE

Switch	Pass-through Power
Catalyst 2960-C	30.8 W
Catalyst 3560-C	22.4 W

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 W*ireless *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.

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation and Submitting a Service Request" section.