Release Notes for the Catalyst 3750, 3560, and 2960 Switches, Cisco IOS Release 12.2(53)SE and Later

Revised August 18, 2010

Cisco IOS Release 12.2(53)SE and later runs on all Catalyst 3750 and 3560, and 2960 switches and on Cisco EtherSwitch service modules.

Note Cisco IOS Release 12.2(53)SE1 does not support the Cisco EtherSwitch service modules.

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. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(53)SE and later and any limitations, restrictions, and caveats that apply to 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 7.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 8.

For the complete list of Catalyst 3750and 3560, and 2960 switch documentation and of Cisco EtherSwitch service module documentation, see the "Related Documentation" section on page 67.

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

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

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

Contents

This information is in the release notes:

System Requirements

The system requirements are described in these sections:

- Hardware Supported, page 2
- Device Manager System Requirements, page 6
- Cluster Compatibility, page 6
- CNA Compatibility, page 7

Hardware Supported

Table 1 lists the hardware supported on this release.

Table 1 Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware

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 3750-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE

Table 1 Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750-48TS	48 10/100 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-12S	12 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-16TD	16 10/100/1000 Ethernet ports and 1 XENPAK 10-Gigabit Ethernet module slot	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24PS	24 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24TS-1U	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750V2-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-48PS	48 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-48TS	48 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560-8PC	8 10/100 PoE ports and 1 dual-purpose port[3] (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 3560-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-48TS	48 10/100 ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24PS	24 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-12PC Compact Switch	12 Ethernet 10/100 ports with PoE and 1 dual-purpose 10/100/1000 or SFP uplink	Cisco IOS Release 12.2(50)SE
Catalyst 3560V2-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-48PS	48 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-48TS	48 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-24TS-SD	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(50)SE1

Table 1 Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware

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
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

Table 1 Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
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
NME-16ES-1G[4]	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
SFP modules (Catalyst 3750 and 3560)	1000BASE-CWDM[5], -LX, SX, -T, -ZX 100BASE-FX MMF[6] Support for eight additional DWDM SFP optical modules. For a complete list of supported SFPs and part numbers, see the data sheet at: 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	Cisco IOS Release 12.2(25)FX
XENPAK modules[7]	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] PoE = Power over Ethernet

[2] SFP = small form-factor pluggable

3. 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.
4. Cisco EtherSwitch service module
5. CWDM = coarse wavelength-division multiplexer
6. MMF = multimode fiber
7. XENPAK modules are only supported on the Catalyst 3750G-16TD switches.

Device Manager System Requirements

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

- Hardware Requirements, page 6
- Software Requirements, page 6

Hardware Requirements

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

Table 2 Minimum Hardware Requirements

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

[1] We recommend 1 GHz.

[2] We recommend 1 GB DRAM.

Software Requirements

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

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

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

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 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

These are the procedures for downloading software. Before downloading software, read this section for important information:

- Finding the Software Version and Feature Set, page 7
- Deciding Which Files to Use, page 8
- Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility, page 10
- Archiving Software Images, page 10
- Upgrading a Switch by Using the Device Manager or Network Assistant, page 11
- Upgrading a Switch by Using the CLI, page 11
- Recovering from a Software Failure, page 12

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 [formerly known as the SMI] or IP services image [formerly known as the EMI]) 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.

For the Catalyst 3750 and 3560 switches, Cisco IOS Release 12.2(25)SEA and earlier referred to the image that provides Layer 2+ features and basic Layer 3 routing as the standard multilayer image (SMI). The image that provides full Layer 3 routing and advanced services was referred to as the enhanced multilayer image (EMI).

Cisco IOS Release 12.2(25)SEB and later refers to the SMI as the *IP base* image and the EMI as the *IP services* image.

Table 3 lists the different file-naming conventions before and after Cisco IOS Release 12.2(25)SEB.

Table 3 Cisco IOS Image File Naming Convention

Cisco IOS 12.2(25)SEA and earlier	Cisco IOS 12.2(25)SEB and later
c3750-i9-mz (SMI[1])	c3750-ipbase-mz
c3750-i9k91-mz (SMI)	c3750-ipbasek9-mz
c3750-i5-mz (EMI[2])	c3750-ipservices-mz
c3750-i5k91-mz (EMI)	c3750-ipservicesk9-mz
c3560-i9-mz (SMI)	c3560-ipbase-mz
c3560-i9k91-mz (SMI)	c3560-ipbasek9-mz
c3560-i5-mz (EMI)	c3560-ipservices-mz
c3560-i5k91-mz (EMI)	c3560-ipservicesk9-mz

[1] SMI = standard multilayer image

[2] EMI = enhanced multilayer image

Table 4 lists the filenames for this software release.

Table 4 Cisco IOS Software Image Files

Filename	Description
c3750-ipbase-tar.122-53.SE1.tar	Catalyst 3750 IP base image and device manager files. This image has Layer 2+ and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipbaselm-tar.122-53.SE1.tar	Catalyst 3750 IP base image (noncryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c3750-ipbasek9-tar.122-53.SE1.tar	Catalyst 3750 IP base cryptographic image and device manager files. This image has the Kerberos, SSH[1], Layer 2+, and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipbaselmk9-tar.122-53.SE1.tar	Catalyst 3750 IP base image (cryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.

Table 4 Cisco IOS Software Image Files (continued)

Filename	Description
c3750-ipservices-tar.122-53.SE1.tar	Catalyst 3750 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipserviceslm-tar.122-53.SE1.tar	Catalyst 3750 IP services image (noncryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c3750-ipservicesk9-tar.122-53.SE1.tar	Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipserviceslmk9-tar.122-53.SE1.tar	Catalyst 3750 IP services image (cryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c3560-ipbase-tar.122-53.SE1.tar	Catalyst 3560 IP base image file and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3560-ipbaselm-tar.122-53.SE1.tar	Catalyst 3560 IP base image (noncryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c3560-ipbasek9-tar.122-53.SE1.tar	Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3560-ipbaselmk9-tar.122-53.SE1.tar	Catalyst 3560 IP base image (cryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c3560-ipservices-tar.122-53.SE1.tar	Catalyst 3560 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3560-ipserviceslm-tar.122-53.SE1.tar	Catalyst 3560 IP services image (noncryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c3560-ipservicesk9-tar.122-53.SE1.tar	Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3560-ipserviceslmk9-tar.122-53.SE1.tar	Catalyst 3560 IP services image (cryptographic image) with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.
c2960-lanbase-tar.122-53.SE1.tar	Catalyst 2960 image file and device manager files. This image has Layer 2+ features.
c2960-lanbasek9-tar.122-53.SE1.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanlite-tar.122-53.SE1.tar	Catalyst 2960 LAN lite image file and device manager files.
c2960-lanlitek9-tar.122-53.SE1.tar	Catalyst 2960 LAN lite cryptographic image file and device manager files.

[1] SSH = Secure Shell.

Catalyst 3750 or 3560 switches with a 16-MB flash memory can experience problems due to flash memory constraints, especially if they are using larger size images, such as c3750-ipservicesk9-tar, c3560-ipservicesk9-tar, c3750-ipbasek9-tar, or c3750-ipbasek9-tar images. These are the affected switches:

Catalyst 3560: WS-C3560-24PS and WS-C3560-48PS

Catalyst3750: WS-C3750-24PS, WS-C3750-24TS, WS-C3750-48PS, WS-C3750-48TS, WS-3750G-24T, WS-C3750G-12S, WS-C3750G-24TS, WS-C3750G-16TD

The workaround for these switches is to use the corresponding *lm* images, such as the c3750-ipserviceslmk9-tar or c3560-ipserviceslmk9-tar images, which require less memory. In future releases, images are expected to grow more in size, requiring more need for the *lm* images.

Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility

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

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

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

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

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

For information about the controller software, see the release notes on this page for Cisco Software Release 4.0.x.0 or later:

http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

For controller software upgrade procedure, see the *Cisco Wireless LAN Controller Configuration Guide* on this page:

.http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

Archiving Software Images

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

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

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

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

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.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 4 on page 8 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

To download the image for a Catalyst 2960 switch, click **Catalyst 2960 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2960 3DES Cryptographic Software**.

To download the IP services image or IP base image files for a Catalyst 3560 switch, click **Catalyst 3560 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560 3DES Cryptographic Software**.

To download the IP services image or IP base image files for a Catalyst 3750 switch, click **Catalyst 3750 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750 3DES Cryptographic Software**.

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.

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 additional recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

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

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

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

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

New Features

This section describes the new and updated software features provided in this release:

New Software Features

- Support for the cewNeighborLevelTable table and for new MIB objects in the cewEntTable and cewNeighborTable tables in the CISCO-ENERGYWISE-MIB. For information, see the MIB.
- Smart Install enhancements
  - When the director is the TFTP server, you can store the default image and configuration file in the director flash, and the director automatically creates the image_list file.
  - For zero-touch downloads to switches running releases earlier than 12.2(52)SE, the director automatically creates the tailored configuration file.
- Support for the **ip vrf forwarding** *vrf-name* server-group configuration and the **ip radius source-interface** global configuration VRF-Aware RADIUS commands. For more information, see the "Updates to the Catalyst 3750 and 3560 Software Configuration Guides" section on page 48.

Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release required to support the major features of the Catalyst 3750 3560,and 2960 switches and the Cisco EtherSwitch service modules.

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Smart Install to allow a single point of management (director) in a network. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches.	12.2(52)SE	3750, 3560, 2960
Support for IP source guard on static hosts.	12.2(52)SE	3750, 3560, 2960
AutoSmartPort enhancements, which add support for macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros as well as for automatic configuration based on these two new device types: Cisco Digital Media Player (Cisco DMP) and Cisco IP Video Surveillance Camera (Cisco IPVSC).	12.2(52)SE	3750, 3560,2960
RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.	12.2(52)SE	3750, 3560,2960
IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.	12.2(52)SE	3750, 3560, 2960
Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.	12.2(52)SE	3750, 3560, 2960
Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication.	12.2(52)SE	3750, 3560, 2960
Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.	12.2(52)SE	3750, 3560, 2960
VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.	12.2(52)SE	3750, 3560, 2960
MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.	12.2(52)SE	3750, 3560, 2960

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.	12.2(52)SE	3750, 3560, 2960
Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.	12.2(52)SE	3750, 3560, 2960
DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE	3750, 3560,2960
Increased support for LLPD-MED by allowing the switch to grant power to the power device (PD), based on the power policy TLV request.	12.2(52)SE	3750, 3560, 2960
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE	3750, 3560, 2960
Support for IPv6 QoS trust capability.	12.2(52)SE	3750, 3560
Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.	12.2(52)SE	3750, 3560
Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.	12.2(52)SE	3750, 3560
Cisco EnergyWise to manage the power usage of EnergyWise entities, such as power over Ethernet (PoE) devices and end points running EnergyWise agents. **Note** When you use the EnergyWise end-point software development kit (SDK) or the management application programming interface (API), we recommend that the switch runs Cisco IOS Release 12.2(53)SE2 or later.	12.2(53)SE1	3750, 3560, 2960
Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch	12.2(50)SE	3750, 3560, 2960
IEEE 802.1x with open access to allow a host to access the network before being authenticated	12.2(50)SE	3750, 3560, 2960
IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch	12.2(50)SE	3750, 3560, 2960
Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host	12.2(50)SE	3750, 3560, 2960

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port	12.2(50)SE	3750, 3560, 2960
Cisco EnergyWise manages the energy usage of power over Ethernet (PoE) entities	12.2(50)SE	3750, 3560, 2960
Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE)	12.2(50)SE	3750, 3560, 2960
CPU utilization threshold trap monitors CPU utilization	12.2(50)SE	3750, 3560, 2960
Support for the Cisco IOS Configuration Engine, previously referred to as the Cisco IOS CNS agent	12.2(50)SE	3750, 3560, 2960
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode	12.2(50)SE	3750, 3560, 2960
RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group	12.2(50)SE	3750, 3560, 2960
Auto Smartports Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port	12.2(50)SE	3750, 3560, 2960
Support for: SCP attribute 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 supports dynamic routing protocols 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
These IPv6 features are now supported in the IP services and IP base software 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
Support for 802.1x authentication with restricted VLANs (also known as *authentication failed VLANs*) in all switch images	12.2(50)SE	2960
IP source guard restricts traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings	12.2(50)SE	2960
Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN	12.2(50)SE	2960
Generic message authentication support with the SSH Protocol and compliance with RFC 4256	12.2(46)SE	3750, 3560, 2960
Generic message authentication support	12.2(46)SE	3750, 3560, 2960
Disabling MAC address learning on a VLAN	12.2(46)SE	3750, 3560, 2960

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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
Exclude a port in a VLAN from the SVI line-state up or down 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 (requires the advanced IP services image)	12.2(46)SE	3750, 3560
DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image)	12.2(46)SE	3750, 3560
Embedded event manager (EEM) for device and system management (IP services image only)	12.2(46)SE	3750, 3560
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)	12.2(46)SE	2960
Monitor and police the 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
Simple Network and Management Protocol (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
Support for 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 multidomain authentication (MDA)-enabled ports	12.2(40)SE	3750, 3560

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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 these IP services: 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
Support for 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 to test the hardware functionality of the supervisor engine	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 in the IP base and IP services image	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

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Access SDM templates	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 ACLs	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 Multicast Listener Discovery (MLD) snooping	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
QoS hierarchical policy maps on a port	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
NAC Layer 2 IEEE 802.1x validation	12.2(25)SED	3750, 3560, 2960 Cisco EtherSwitch service modules
NAC Layer 2 IP validation	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x inaccessible authentication bypass.	12.2(25)SED 12.2(25)SEE	3750, 3560 Cisco EtherSwitch service module 2960
IEEE 802.1x with restricted VLAN	12.2(25)SED	3750, 3560, 2960 Cisco EtherSwitch service modules
Budgeting power for devices connected to PoE ports	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEC 12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules 2960
Unique device identifier (UDI)	12.2(25)SEC 12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules 2960

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
VRF Lite	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x with wake-on-LAN	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Nonstop forwarding (NSF) awareness	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
Configuration logging	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Secure Copy Protocol	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Cross-stack EtherChannel	12.2(25)SEC	3750 Cisco EtherSwitch service modules
Support for configuring private-VLAN ports on interfaces that are configured for dynamic ARP inspection (IP base image [formerly known as the SMI] only)	12.2(25)SEB	3750, 3560
Support for IP source guard on private VLANs (IP base image [formerly known as the SMI] only)	12.2(25)SEB	3750, 3560
Support for configuring an 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
Support for DSCP transparency	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
Support for 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

Table 5 Catalyst 3750 and 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Layer 2 point-to-point tunneling and Layer 2 point-to-point tunneling bypass	12.2(25)SE	3750, 3560
Support for SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
Support for configuring private-VLAN ports on interfaces that are configured for dynamic ARP inspection (IP services image [formerly known as the EMI] only)	12.2(25)SE	3750, 3560
Support for IP source guard on private VLANs (IP services image [formerly known as the EMI] only)	12.2(25)SE	3750, 3560
Cisco intelligent power management to limit the power allowed on a port, or pre-allocate (reserve) power for a port.	12.2(25)SE	3750, 3560
IEEE 802.1x accounting and MIBs (IEEE 8021-PAE-MIB and CISCO-PAE-MIB)	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Dynamic ARP inspection	12.2(20)SE	3750, 3560
Flex Links	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Software upgrade (device manager or Network Assistant only)	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
IP source guard	12.2(20)SE	3750, 3560
Private VLAN (IP services image [formerly known as the EMI] 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.

This section contains these limitations:

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

These are the configuration limitations:

- 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)

- 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)

- 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)

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

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

  There is no workaround. (CSCed95822)

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

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

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

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

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

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

  There is no workaround. (CSCeh50152)

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

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

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

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

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)

- 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).

- 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)
- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)
- When the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as `up` and sometimes as `down`, resulting in conflicts. This status depends on when you respond to the reboot query:

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

  The workaround is to wait for approximately 1 minute after rebooting and until the VLAN 1 interface line status appears on the console before you respond to the query. (CSCsl02680) (Catalyst 3750 and 3560 switches)
- A T-start error message appears after startup under these conditions:
  - Two-link ports on the same switch are connected with a crossover cable.
  - The switch is running Cisco IOS 12.2(50)SE3 or later.

  The workaround is to connect the two ports with a straight-through cable. (CSCsr41271) (Catalyst 3750V2 and Catalyst 3560V2 PoE switches and Cisco Etherswitch service modules only)
- If you enter the **show tech-support** privileged EXEC command after you enter the **remote command** {**all** | *stack-member-number*} privileged EXEC command, the complete output does not appear.

  The workaround is to use the **session** *stack-member-number* privileged EXEC command. (CSCsz38090)
- When authorization and accounting are enabled on the switch and you use the interface range command to change the configuration on a range of interfaces, the change might cause high CPU utilization and authentication failures.

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

Ethernet

These are the Ethernet limitations:

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

  These are the workarounds:

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

  For more information, enter *CSCea77032* in the Bug Toolkit at this URL:

  http://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

These are the fallback bridging limitations:

- (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

This is the Hot Standby Routing Protocol (HSRP) limitation:

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

These are the IP limitations:

- (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

These are the IP telephony limitations:

- 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

This is the MAC addressing limitation:

(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

These are the multicasting limitations:

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

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

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

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

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

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

  Use one of these workarounds:

  - Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)

- If IP routing is disabled and IP multicast routing is enabled on a switch running Cisco IOS Release 12.2(25)SED, IGMP snooping floods multicast packets to all ports in a VLAN.

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

- A switch drops unicast traffic under these conditions:
  - The switch belongs to a Layer 2 ring.
  - More than 800 Mbps of multicast traffic is sent in both directions on the interface.

  When multicast traffic is sent in one direction and unicast traffic is sent in another, unicast traffic is dropped at the multicast traffic source port.

  The workaround is to apply a policy map so that the least significant traffic is discarded. (CSCsq83882)

Power

These are the powers limitation for the Cisco EtherSwitch service modules:

- 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

These are the quality of service (QoS) limitations:

- 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)

RADIUS

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

  There is no workaround. (CSCta05071)

Routing

These are the routing limitations:

- (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)

SPAN and RSPAN

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

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

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

  - 3560-24PS
  - 3560-48PS
  - 3750-24PS
  - 3750-48PS
  - 3750-24TS
  - 3750-48TS
  - 3750G-12S
  - 3750G-24T
  - 3750G-24TS
  - 3750G-16TD
  - Cisco EtherSwitch service modules
- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround.

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

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

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

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

  - 3560-24PS
  - 3560-48PS
  - 3750-24PS
  - 3750-48PS
  - 3750-24TS
  - 3750-48TS
  - 3750G-12S
  - 3750G-24T
  - 3750G-24TS
  - 3750G-16TD
  - Cisco EtherSwitch service modules
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)
- On Catalyst 3750 switches running Cisco IOS Release 12.1(14)EA1 and later, on Catalyst 3560 switches running Cisco IOS release 12.1(19)EA1 or later, or on Cisco EtherSwitch service modules, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)
- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

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

These are the Catalyst 3750 and Cisco EtherSwitch service module switch stack limitations:

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)
- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual bootup is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots. There is no workaround. (CSCec36644)
- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mb/s egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch (such as a Catalyst 3750-24TS or 3750-48TS switch) than if it is on a Gigabit Ethernet switch (such as a Catalyst 3750G-24T or 3750G-24TS switch). There is no workaround. (CSCed00328)
- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost. The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)
- When the **switchport** and **no switchport** interface configuration commands are entered more than 20,000 times on a port of a Catalyst 3750 switch or on a Cisco EtherSwitch service module, all available memory is used, and the switch halts.

  There is no workaround. (CSCed54150)
- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master re-election occurs on one of the Catalyst 3750 or Cisco EtherSwitch service module default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master re-election cannot complete.

  The workaround is to complete the MAC address update by entering the **clear arp** privileged EXEC command. (CSCed62409)
- When a Catalyst 3750 switch or Cisco EtherSwitch service module is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded. There is no workaround. (CSCed70894)
- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the IP base image (formerly known as the SMI) and the old stack master was running the IP services image (formerly known as the EMI).

  Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the IP services image (formerly known as the EMI) or the IP base image (formerly known as the SMI):

  - If the stack master is running the IP services image (formerly known as the EMI), all stack members have private VLAN enabled.
  - If the stack master is running the IP base image (formerly known as the SMI), 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 (formerly known as the EMI) and the new stack master is running the IP base image (formerly known as the SMI). 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 (formerly known as the EMI) to IP base image (formerly known as the SMI) master switch change (or the reverse).
  - Before an IP services image (formerly known as the EMI)-to-IP base image (formerly known as the SMI) 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)

- 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)

Trunking

These are the trunking limitations:

- 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

These are the VLAN limitations:

- 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)

Device Manager Limitations

These are the device manager limitations:

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

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

Important Notes

These sections describe the important notes related to this software release for the Catalyst 3750 and3560, and 2960 switches and for the Cisco EtherSwitch service modules:

- Switch Stack Notes, page 38
- Cisco IOS Notes, page 38
- Device Manager Notes, page 39

Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- Catalyst 3560 switches do not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because these switches share common code with other switches that do support stacking.
- Catalyst 3750 switches running Cisco IOS Release 12.2(25)SEB are compatible with Cisco EtherSwitch service modules running Cisco IOS Release 12.2(25)EZ. Catalyst 3750 switches and Cisco EtherSwitch service modules can be in the same switch stack. In this switch stack, the Catalyst 3750 switch or the Cisco EtherSwitch service module can be the stack's active switch.
- The LED of a switch port blinks amber if MDA is configured, there is no phone behind the IP phone, and the default **authentication control-direction both** command is used. This is because the data vlan spanning-tree is not in forwarding the state, which causes the LED to blink in amber.

Cisco IOS Notes

These notes apply to Cisco IOS software:

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

  In Cisco IOS Release 12.2(18)SE and later, you can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)
- In Cisco IOS Release 12.2(25)SEC for the Catalyst 3750 and 3560 switches and in Cisco IOS Release 12.2(25)SED for the Catalyst 2960 switch, the implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

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

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

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

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

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

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

Device Manager Notes

These notes apply to the device manager:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- 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 severity 3 Cisco IOS configuration caveats apply to the Catalyst 3750 and 3560, and 2960 switches and to Cisco EtherSwitch service modules:

- CSCeh01250 (Cisco EtherSwitch service modules)

  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.

- CSCeh52964 (Cisco EtherSwitch service modules)

  When the router is rebooted after it is powered on (approximately once in 10 to 15 reboots), the Router Blade Communication Protocol (RBCP) between the router and the EtherSwitch service module might not be reestablished, and this message appears:

  ```
  [date]: %Y88E8K-3-ILP_MSG_TIMEOUT_ERROR: GigabitEthernet1/0: EtherSwitch Service
  Module RBCP ILP messages timeout
  ```

  The workaround is to reload the EtherSwitch service module software without rebooting the router. You can reload the switching software by using the **reload** user EXEC command at the EtherSwitch service module prompt or by using the **service-module g** *slot_numer /0* **reset** privileged EXEC command at the router prompt.

- CSCsx38711 (Catalyst 3750 switches)

  When a port is configured for single host mode, and the re-authentication timer value is less than 100, if the access control server (ACS) is configured with a per-user access control list (ACL), multiple changes to the stack master might cause the display of empty access-lists for the port.

  The workaround is to enter a **shutdown** and then a **no shutdown** interface configuration command on the interface.

- CSCsx70643 (Catalyst 3750 switches)

  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.

- CSCsy85676

  When you configure an ACL and enter the **access-group** interface configuration command to apply it to an interface for web authentication, the output from the **show epm session ip-address** or **show ip access_list interface** *interface-id* privileged EXEC command does not show any web authentication filter ID.

  There is no workaround.

- CSCsy88966 (Catalyst 3750G-16TD switches running Cisco IOS Release 12.2(46)SE or later)

  If you insert a XENPAK module in the switch module slot, the slot LED turns green before you connect the cable.

  There is no workaround.

- CSCtb08823 (Catalyst 3750 switches)

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

  There is no workaround.

- CSCtc02635

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

  There is no workaround.

- CSCtc91312

  EnergyWise is enabled and you use the **energywise level** *level* **recurrence importance** *importance* **at** *minute hour day_of_month month day_of_week* interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might

  - Restart when it tries to power a PoE device
  - Power on or off the PoE device at an incorrect time
  - Fail

  This occurs when the time change for the next year occurs after the time change for the current year.

  Before the time change occurs, use one of these workarounds:

  - Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
  - Use the **energywise level** *level* **recurrence importance** *importance* **time-range** *time-range-name* interface configuration command to reschedule the events.
  - Use the **power inline auto** interface configuration command to power on the PoE port.

- CSCtd29049

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

  There is no workaround.

- CSCtf28627 (Catalyst 2960 switches)

  When you add 4000 VLAN instances to a Cisco Catalyst 2960 switch that functions as a VLAN Trunking Protocol version 3 (VTPv3) server, memory fragmentation can occur and cause the switch to fail.

  Workaround: Do not configure more than 255 VLANs on a Cisco Catalyst 2960 switch that functions as a VTPv3 server.

- CSCtd81955

  When you configure more than one EnergyWise domain in a Layer 2 broadcast domain, IP connectivity to the switch might be lost, high CPU usage might occur on the switch, and a broadcast storm might occur in the subnet.

  The workaround is to configure only a single EnergyWise domain in the Layer 2 broadcast domain.

- CSCtf31741

  Orchestrator shows a previously discovered stack as ‘not checking in’ and discovers a new previously unseen stack. This condition occurs when you remove the master of a switch stack, causing the remaining stack members to elect a new stack master, and, in turn, causing the EnergyWise IDs to change.

  There is no workaround.

Resolved Caveats

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(53)SE2

- CSCte96453

  A switch fails when you enter the **energywise level 10** interface configuration command on a Power-over-Ethernet (PoE) port.

  There is no workaround.

- CSCtf59354

  When a device is connected to a Fast Ethernet port on a Cisco EtherSwitch service module that is running Cisco IOS Release 12.2(53)SE or later, the port flaps and then changes to error-disabled.

  The workaround is to enter the **power inline never** interface configuration command.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(53)SE1

- CSCsx29696 (Catalyst 2960 switches)

  On a switch running Cisco IOS Release 12.2(35)SE or later, connectivity issues might occur with these messages:

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

- CSCsx97605

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

- CSCsz18634 (Catalyst 2960 switches)

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

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

- CSCtb10158

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

  There is no workaround.

- CSCtc02635 (Catalyst 2960 switches)

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

  There is no workaround.

- CSCtc16848 (Catalyst 2960 switches)

  The output of the **show inventory** user EXEC command sometimes does not display all of the connected SFP modules. The EntitityMIB does not report these SFP modules.

  This occurs intermittently on the 3560-48TS, C3560-48PS, and C3560G-48PS switches. There is no workaround.

- CSCtc43231

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

  There is no workaround.

- CSCtc53453 (Catalyst 3750 switches)

  If you configure EnergyWise on a member switch and then restart it by entering the **reload slot** *stack-member-number* privileged EXEC command, the EnergyWise configuration is removed from the switch.

  The workaround is to save the switch configuration by using the **copy running-configuration startup-configuration** privileged EXEC command and then restart the switch stack.

- CSCtc57809 (Catalyst 2960 switches)

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

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

  There is no workaround.

- CSCtc59162

  Modifying a prefix list that is configured as an inbound or outbound distribute-list causes the EIGRP peer to resynchronize.

- CSCtc71798 (Catalyst 3750 switches)

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

- CSCtd31242 (Catalyst 2960 switches)

  An IP phone loses network connectivity under these conditions:

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

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

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

- CSCtd72456 (Catalyst 2960 switches)

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

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

- CSCtd83311 (Catalyst 3560 and 2960 switches)

  After you have entered the **speed nonegotiate** interface configuration command and restarted a switch that is running Cisco IOS Release 12.2(52)SE, UniDirectional Link Detection (UDLD) can enter an unknown state on a dual-purpose port with a Serial Gigabit Media Independent Interface (SGMII) connection.

These switches could be affected:

  - WS-C3560-8PC
  - WS-C3560-12PC-S
  - WS-C2960-24LC-S
  - WS-C2960-24PC-L
  - WS-C2960-24PC-S
  - WS-C2960-8TC-L
  - WS-C2960-24TC-L
  - WS-C2960-48TC-L
  - WS-C2960-8TC-S
  - WS-C2960-24TC-S
  - WS-C2960-48TC-S
  - WS-C2960G-8TC-L
  - WS-C2960G-24TC-L
  - WS-C2960G-48TC-L

Workaround: Enter the **no speed** interface configuration command, enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface configuration command.

- CSCte52821

  When you enter the **no ip ftp passive** global configuration command to allow all types of FTP connections on a switch running Cisco IOS Release 12.2(52)SE or 12.2(53)SE, FTP sessions could disable Telnet or console connections. Then you can no longer use the vty.

  Workaround: When you cannot use the vty, restart the switch. To prevent FTP sessions from disabling Telnet or console connections, enter the **ip ftp passive** global configuration command.

- CSCte54884 (Catalyst 3750 and 3560 switches)

  A switch that runs Cisco IOS Release 12.2(53)SE can fail when you enable dot1x authentication.

  There is no workaround.

- CSCte67201

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

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

- CSCte72365

  After upgrading from Cisco IOS 12.2(52)SE to Cisco IOS 12.2(53)SE, EIGRP hello packets are flooded on access ports of other subnets. This also occurs when pings are sent to the broadcast address of other subnets.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(53)SE

- CSCsj68446

  The Network Time Protocol (NTP) might not synchronize when the switch is configured as an NTP client. These are the two possible workarounds:

  - Enter the **no ntp** global configuration command twice.
  - Reconfigure NTP on the port. For more information, see the “Configuring NTP” section of the “Administering the Switch” chapter in the software configuration guide.

- CSCsx29696

  On switches running Cisco IOS release 12.2(35)SE or later, connectivity issues might occur with these messages:

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

  There is no workaround.

- CSCsz18634

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

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

- CSCtb62629 (Catalyst 3750 and 3560 switches)

  A Catalyst 3750V2 or Catalyst 3560V2 switch does not supply inline power to PoE devices when the switch is cold-booted from RPS DC power, that is after you disconnect all power to the switch and then reconnect RPS power.

  This problem is seen only on Catalyst 3560V2 or 3750V2 switches, not on non-V2 switches.

  The workaround is to configure a soft reload of the switch by entering the **reload** privileged EXEC command. This causes the inline power to work, even when the RPS is the only source of power.

- CSCtc02635

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

  There is no workaround.

- CSCtc16848

  The output of the **show inventory** user EXEC command sometimes does not display all of the connected SFP modules. The EntitityMIB does not report these SFP modules.

  This occurs intermittently on the 3560-48TS, C3560-48PS, and C3560G-48PS switches. There is no workaround.

- CSCtc20603

  If IEEE 802.1Q native VLAN tagging is enabled on a switch, PDUs sent from an EtherChannel in LACP mode are tagged.

  There is no workaround.

- CSCtc30872

  When a BPDU guard is globally enabled on a switch and the access VLAN is a VLAN other than VLAN 1, BPDU guard does not run on a multiple VLAN access port.

  The workaround is to enable BPDU guard on the port.

- CSCtc57809

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

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

  There is no workaround.

- CSCtc67421

  When 24 phones connected to PoE ports start at the same time, LLDP for power management fails.

  The workaround is to start the phones one at a time. This might not work after a power outage or other power failure event.

- CSCtd31242

  An IP phone loses network connectivity under these conditions:

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

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

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

- CSCtd72456

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

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

Documentation Updates

Updates to the Catalyst 3750 and 3560 Software Configuration Guides

Updates for the "Unsupported Commands" Appendix

Beginning with Cisco IOS Release 12.2(35)SE5, these commands are supported and should be removed from this appendix:

- **set as-path** (route-map command)
- **set tag** (route-map configuration)
- **ip prefix-list** (global configuration)
- **ip as-path access-list** (global configuration)

Beginning with Cisco IOS Release 12.2(40)SE, this IP multicast routing command is supported and should be removed from this appendix:

- **ip igmp helper-address** *ip-address* (interface configuration command)

New Section for the "Configuring IP Unicast Routing" Chapter

User Interface for VRF-Aware RADIUS

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. This release supports the **ip vrf forwarding** *vrf-name* server-group configuration and the **ip radius source-interface** global configuration commands, as described in the *Per VRF AAA Feature Guide* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

New Information for the "Overview" Chapter

Availability and Redundancy Features

RPS support through the Cisco Redundant Power System 2300, also referred to as the RPS 2300, for enhancing power reliability, configuring and managing the redundant power system. For more information about the RPS 2300, see the *Cisco Redundant Power System 2300 Hardware Installation Guide* that shipped with the device and that is also on Cisco.com.

New Information for the "Configuring Switch Stacks" Chapter

Hardware Loopback

On Catalyst 3750V2 members, the *Loopback HW* value is always *N/A*.

Configuring the Cisco Redundant Power System 2300

Follow these guidelines:

- The RPS name is a 16-character-maximum string.
- On a Catalyst 3560V2 or a standalone Catalyst 3750V2 switch, the RPS name applies to the connected RPS 2300.
- In a switch stack, the RPS name applies to the RPS ports connected to the specified switch.

- If you do not want the RPS 2300 to provide power to a switch, but do not want to disconnect the cable between the switch and the RPS 2300, use the **power rps** *switch-number* **port** *rps-port-id* **mode standby** user EXEC command.
- You can configure the priority of an RPS 2300 port from 1 to 6. A value of 1 assigns highest priority to a port and its connected device. A value of 6 assigns lowest priority to a port and its connected device.
- If multiple switches connected to the RPS 2300 need power, the RPS 2300 powers those with the highest priority. It applies any other available power to the lower-priority switches.

Beginning in user EXEC mode:

	Command	Purpose
Step 1	**power rps** *switch-number* **name** {*string* | **serialnumber**}	Specify the name of the RPS 2300. The keywords have these meanings: • *switch-number*—Specify the stack member to which the RPS 2300 is connected. The range is 1 to 9, depending on the switch member numbers in the stack. This keyword is supported only on Catalyst 3750V2 switches. • **name**—Set the name of the RPS 2300, and enter one of these options: – *string*—Specify the name, such as *port1* or *“port 1”*. Using quotation marks before and after the name is optional, but you must use quotation marks if you want to include spaces in the port name. The name can have up to 16 characters. – **serialnumber**—Configure the switch to use the RPS 2300 serial number as the name.
Step 2	**power rps** *switch-number* **port** *rps-port-id* **mode** {**active** | **standby**}	Specify the mode of the RPS 2300 port. The keywords have these meanings: • *switch-number*—Specify the stack member connected to the RPS 2300. The range is 1 to 9, depending on the switch member numbers in the stack. This keyword is supported only on Catalyst 3750V2 switches. • **port** *rps-port-id*—Specify the RPS 2300 port. The range is from 1 to 6. • **mode**—Set the mode of the RPS 2300 port: – **active**—The RPS 2300 can provide the power to a switch when the switch internal power supply cannot. – **standby**—The RPS 2300 is not providing power to a switch. The default mode for RPS ports is **active**.

	Command	Purpose
Step 3	**power rps** *switch-number* **priority** *priority*	Set the priority of the RPS 2300 port. The range is from 1 to 6, where 1 is the highest priority and 6 is the lowest priority. The default port priority is 6.
Step 4	**show env rps**	Verify your settings.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default name setting (no configured name), use the **power rps** *switch-number* **port** *rps-port-id* **name** user EXEC command with no space between the quotation marks.

To return to the default port mode, use the **power rps** *switch-number* **port** *rps-port-id* **active** command.

To return to the default port priority, use the **power rps** *switch-number* **port** *rps-port-id* **priority** command.

For more information about using the **power rps** user EXEC command, see the command reference for this release.

Monitoring Interface Status

In the "Show Commands for Interfaces" table, the **show env rps** privileged EXEC command shows any connected redundant power system (RPS).

- Catalyst 3750-E or 3560-E switch—Only the Cisco Redundant Power System 2300, also referred to as the RPS 2300.
- Catalyst 3750V2 or 3560V2 switch—Only the RPS 2300.
- Catalyst 3750, 3560 switches—RPS 2300 or Cisco RPS 675 Redundant Power System, also referred to as the RPS 675.

Updates to the Software Configuration Guides

This section was added to the "Configuring IEEE 802.1x Port-Based Authentication" chapter of all the software configuration guides:

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

This guideline was added to the “802.1x Authentication” section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter.

- When IP phones are connected to an 802.1x-enabled switch port that is in single host mode, the switch grants the phones network access without authenticating them. We recommend that you use multidomain authentication (MDA) on the port to authenticate both a data device and a voice device, such as an IP phone.

Note Only Catalyst 3750, 3560, and 2960 switches support CDP bypass. The Catalyst 3750-E and 3560-E switches do not support CDP bypass.

This guideline was added to the “MSTP Configuration Guidelines” section of the “Configuring MSTP” chapter:

- When the switch is in MST mode, it uses the long path-cost calculation method (32 bits) to compute the path cost values. With the long path-cost calculation method, these path cost values are supported:

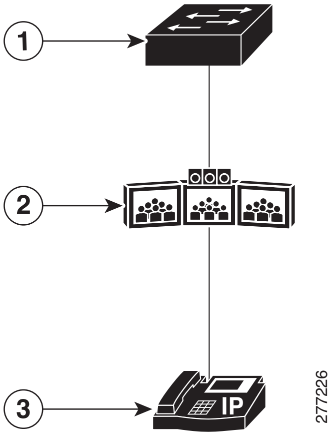
Speed	Path Cost Value
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

The “Configuring TelePresence E911 IP Phone Support” chapter was added to the Catalyst 3750 and 3560 software configuration guides.

Understanding TelePresence E911 IP Phone Support

You can use a Cisco IP phone as a user interface in a Cisco TelePresence System. See in Figure 1. In this configuration, the IP phone must always be on and available for emergency calls. If the power to the codec in the Cisco TelePresence System fails, is disrupted or if the codec fails, the IP phone is not available.

Figure 1 Phone-Codec-Switch Connection



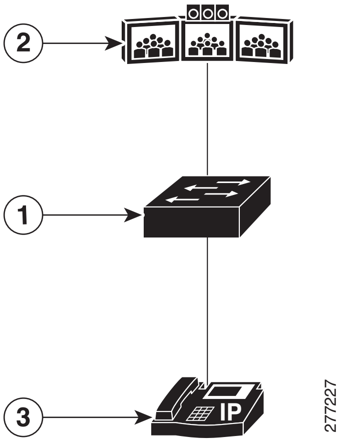
1	Switch	**3**	IP phone
2	Cisco TelePresence System with a codec		

Use the TelePresence E911 IP phone support feature to ensure that the IP phone is always on and available for emergency calls. When a CDP-enabled IP phone is connected to the codec through a switch, you can configure the switch to forward CDP packets from the IP phone only to the codec in the Cisco TelePresence System. The switch adds *ingress-egress port pairs* to the CDP forwarding table. An ingress-egress port pair is a one-to-one mapping between an ingress switch port connected to the IP phone and an egress switch port connected to the codec.

The IP phone and the codec communicate through the IP network. If power to the codec fails, is disrupted or if the codec fails, the IP phone is still connected to the IP network and is available for emergency calls.

The switch forwards all CDP packets received on the ingress port to the egress port. If multiple IP phones are connected to the codec through a single port on the switch, only one phone communicates with it through the IP network. This phone is usually the one that sent the first CDP packet received by the codec.

Figure 2 Phone-Switch-Codec Connection



1	Switch	**3**	CDP-enabled IP phone
2	Cisco TelePresence System with a codec		

Configuring TelePresence E911 IP Phone Support

- Configuration Guidelines, page 53
- Enabling TelePresence E911 IP Phone Support, page 53
- Example, page 54

Configuration Guidelines

- You must use only CDP-enabled phones with TelePresence E911 IP phone support.
- You can connect the IP phone and codec in the Cisco TelePresence System through any two ports in a switch stack.

Enabling TelePresence E911 IP Phone Support

Beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**cdp forward ingress** *port-id* **egress** *port-id*	Configures an ingress-egress port pair. • **ingress** *port -id*—Specifies the port connected to the CDP-enabled IP phone. • **egress** *port-id*—Specifies the port connected to the codec in the Cisco TelePresence System. Repeat this step to configure additional ingress-egress port pairs.
Step 3	**end**	Returns to privileged EXEC mode.

	Command	Purpose
Step 4	**show cdp forward**	Verifies the ingress-egress port pairs. The command output also shows the number of forwarded and dropped packets.
Step 5	**copy running-config startup config**	(Optional) Saves your entries in the configuration file.

Example

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# cdp forward ingress gigabitethernet2/0/1 egress gigabitethernet2/0/12
Switch(config)# cdp forward ingress gigabitethernet2/0/1 egress gigabitethernet2/0/13
Ingress interface already configured
Switch(config)# cdp forward ingress gigabitethernet2/0/2 egress gigabitethernet2/0/12
Egress interface already configured
Switch(config)# cdp forward ingress gigabitethernet2/0/2 egress gigabitethernet2/0/13
Switch(config)# end
Switch#
*Mar  1 13:38:34.954: %SYS-5-CONFIG_I: Configured from console by console
Switch# show running-config | include cdp
cdp forward ingress GigabitEthernet2/0/1 egress GigabitEthernet2/0/12
cdp forward ingress GigabitEthernet2/0/2 egress GigabitEthernet2/0/13
Switch# show cdp forward

Ingress         Egress         # packets         # packets
Port            Port           forwarded         dropped
-------------------------------------------------------------
 Gi2/0/1        Gi2/0/12            0                0
 Gi2/0/2        Gi2/0/13            0                0

Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no cdp forward ingress gigabitethernet2/0/1
Switch(config)# end
Switch#
*Mar  1 13:39:14.120: %SYS-5-CONFIG_I: Configured from console by console
Switch# show running-config | include cdp
cdp forward ingress GigabitEthernet2/0/2 egress GigabitEthernet2/0/13
Switch# show cdp forward
Ingress         Egress         # packets         # packets
Port            Port           forwarded         dropped
-------------------------------------------------------------
 Gi2/0/2        Gi2/0/13            0                0

Switch#
```

Updates to the Command References

These command were added to the Catalyst 3750 and 3560 command references:

- cdp forward, page 55
- show cdp forward, page 56

cdp forward

To specify the ingress and egress switch ports for CDP traffic, use the **cdp forward** global configuration command. To return to the default setting, use the **no** form of this command.

cdp forward ingress *port-id* **egress** *port-id*

no cdp forward ingress *port-id*

Syntax Description

ingress *port-id*	Specifies the switch port that receives the CDP packet from an IP phone.
egress *port-id*	Specifies the switch port that forwards the CDP packet to the Cisco TelePresence System.

Defaults

The default path for CDP packets through the switch is from any ingress port to the egress port connected to the Cisco Telepresence System.

Command Modes

Global configuration

Command History

Release	Modification
12.2(53)SE	This command was introduced.

Usage Guidelines

You must use only CDP-enabled phones with TelePresence E911 IP phone support.

You can connect the IP phone and codec in the Cisco TelePresence System through any two ports in a switch stack.

Examples

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# cdp forward ingress gigabitethernet2/0/1 egress gigabitethernet2/0/12
Switch(config)# cdp forward ingress gigabitethernet2/0/2 egress gigabitethernet2/0/13
Switch(config)# end
Switch# show running-config | include cdp
cdp forward ingress GigabitEthernet2/0/1 egress GigabitEthernet2/0/12
cdp forward ingress GigabitEthernet2/0/2 egress GigabitEthernet2/0/13
Switch# show cdp forward
Ingress         Egress         # packets         # packets
Port            Port           forwarded         dropped
-------------------------------------------------------------
 Gi2/0/1        Gi2/0/12            0                0
 Gi2/0/2        Gi2/0/13            0                0
```

Related Commands

Command	Description
show cdp forward	Displays the CDP forwarding table.

show cdp forward

To display the CDP forwarding table, use the **show cdp forward** user EXEC command.

show cdp forward [**entry** | **forward** | **interface** *interface-id* | **neighbor** | **traffic**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

entry	(Optional) Displays information about a specific neighbor entry.
forward	(Optional) Displays the CDP forwarding information.
interface *interface-id*	(Optional) Displays the CDP interface status and configuration.
neighbor	(Optional) Displays the CDP neighbor entries.
traffic	(Optional) Displays the CDP statistics.
begin	(Optional) Display begins with the line that matches the expression.
exclude	(Optional) Display excludes lines that match the expression.
include	(Optional) Display includes lines that match the specified expression.
expression	(Optional) Expression in the output to use as a reference point.

Command Modes

Use EXEC

Command History

Release	Modification
12.2(53)SE	This command was introduced.

Usage Guidelines

The **show cdp forward** command output shows the number of CDP packets forwarded on each ingress-port- to-egress-port mapping and the statistics for forwarded and dropped packets.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

```
Switch# show cdp forward
Ingress         Egress         # packets         # packets
Port            Port           forwarded         dropped
-------------------------------------------------------------
 Gi2/0/2        Gi2/0/13            0                 0
```

Related Commands

Command	Description
cdp forward	Configures the ingress and egress switch ports for CDP traffic.

Updates to the System Message Guides

This section contains the system message guide updates.

New System Messages

These messages were added to all of the system message guides:

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

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

Recommended Action Reduce other system activity to reduce memory demands.

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

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

Recommended Action No action is required.

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

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

Explanation No action is required.

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

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

Recommended Action No action is required.

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

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

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

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

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

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

Recommended Action Use a different VLAN.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN AuditSessionID [chars]`

Explanation An attempt was made to assign a data VLAN to an IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change either the voice VLAN or the IEEE 802.1x-assigned VLAN on the interface so that they are not the same.

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

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

Explanation Assign a different VLAN.

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

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

Recommended Action Update the configuration to use a valid VLAN.

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

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

Recommended Action Make sure the VLAN exists and is not shutdown or use another VLAN.

Deleted System Messages

These messages were deleted from all of the system message guides:

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

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

Recommended Action Reduce other system activity to reduce memory demands.

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

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

Recommended Action No action is required.

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

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

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

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

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

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

Recommended Action Use a different VLAN.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Recommended Action Multi-Domain Authentication (MDA) host mode cannot start if the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port.

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

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN.`

Explanation An attempt was made to assign a data VLAN to an IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, and [chars] is the port.

Recommended Action Change either the voice VLAN or the IEEE 802.1x-assigned VLAN on the interface so that they are not the same.

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

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

Recommended Action Assign a different VLAN.

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

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

Recommended Action Update the configuration to use a valid VLAN.

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

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

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

Error Message `DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Dot1x cannot assign a VLAN [dec] to a routed port [chars]`

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

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

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

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

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

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

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

Recommended Action Assign a different VLAN.

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

Explanation This message means that remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, and [chars] is the port.

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

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

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

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

Updates to the Catalyst 3750 and 3560, and 2960 Hardware Installation Guide

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

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

These standards provide guidelines for acceptable working environments and acceptable levels of suspended particulate matter:

- Network Equipment Building Systems (NEBS) GR-63-CORE
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20

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

- Catalyst 3560-8PC switch—8 10/100 PoE ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
- Catalyst 2960-8TC switch—8 10/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
- Catalyst 2960G-8TC switch—7 10/100/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)

Updates for the *Catalyst 2960 Switch Hardware Installation Guide*

This update is for the “Overview” chapter. These PoE switches were added:

Table 6 Catalyst 2960 Switch Model Descriptions

Switch Model	Supported Software Image	Description
Catalyst 2960-48PST-S	LAN-Lite	48 10/100 PoE ports, 2 10/100/1000 ports, and 2 SFP module slots
Catalyst 2960-24PC-S	LAN-Lite	24 10/100 PoE ports and 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP module slots)
Catalyst 2960-24LC-S	LAN-Lite	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)

Note The PoE sections in the hardware guide also apply to these switches, even though they are not listed in the hardware guide.

This update is for the “Technical Specifications” chapter.

Table 7 Catalyst 2960-48PST-S, Catalyst 2960-24PC-S, and Catalyst 2960-24LC-S Specifications

Power Requirements	
AC input voltage	100 to 240 VAC (autoranging) 8 to 4 A, 50 to 60 Hz (Catalyst 2960-24PC-S) 3 to 1.5 A, 50 to 60 Hz (Catalyst 2960-24LC-S) 5 to 2 A, 50 to 60 Hz (Catalyst 2960-48PST-S)
DC input voltage for RPS 2300	+ 12 V⎓@11.25 A, –48 V⎓@ 7.8 A (Catalyst 2960-24PC-S) + 12 V⎓@ 8.3 A, –48 V⎓@ 2.7 A (Catalyst 2960-24LC-S) +12 V⎓@ 4 A, –48 V⎓@ 7.8 A (Catalyst 2960-48PST-S)
Power consumption[1]	100 W, 341 BTUs per hour (Catalyst 2960-24PC-S) 51 W, 174 BTUs per hour (Catalyst 2960-24LC-S) 483 W, 1647 BTUs per hour (Catalyst 2960-48PST-S)
Power rating	0.470 KVA (Catalyst 2960-24PC-S) 0.175 KVA (Catalyst 2960-24LC-S) 0.5 KVA (Catalyst 2960-48PST-S)
Power over Ethernet	
15.4 W-per-port maximum, 370-W switch maximum (Catalyst 2960-48PST-S and Catalyst 2960-24PC-S). 15.4 W-per-port maximum, 124-W switch maximum (Catalyst 2960-24LC-S).	
Physical Dimensions	
Weight	12 lb (5.44 kg) (Catalyst 2960-24PC-S) 10 lb (4.54 kg) (Catalyst 2960-24LC-S) 12 lb (5.44 kg) (Catalyst 2960-48PST-S)
Dimensions (H x W x D)	1.73 x 13 x 17.5 in. (4.39 x 33.02 x 44.45 cm)

[1] The power consumption values are for the switch input power.

Update to the Getting Started Guide

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

Correction to the *Getting Started Guide for the Catalyst 2960 Switch*

This correction is for the “Shipping Box Contents” section of localized versions of the getting started guide (for the 24- and 48-port switches).

The console cable is optional and is not included in the box. It is orderable.

Update to the *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch*

This warning applies to the Catalyst 2960 24- and 48-port switches:

Statement 266—Switch Installation Warning

Warning **To comply with safety regulations, mount switches on a wall with the front panel facing up.** Statement 266

Waarschuwing **Om te voldoen aan de veiligheidsvoorschriften dient u de schakelaars op een muur te monteren met het voorpaneel omhoog.**

Varoitus **Turvallisuusmääräykset edellyttävät, että kytkimet kiinnitetään seinään etupaneeli ylöspäin.**

Attention **Pour satisfaire aux dispositions de sécurité, installez les commutateurs muraux avec le panneau frontal vers le haut.**

Warnung **Zur Einhaltung der Sicherheitsvorschriften die Schalter so an einer Wand montieren, dass die Frontplatte nach oben zeigt.**

Avvertenza **In conformità ai regolamenti di sicurezza, installare i dispositivi switch a muro con il pannello frontale rivolto in su.**

Advarsel **For å etterkomme sikkerhetsreglene skal brytere monteres på en vegg med frontpanelet vendt opp.**

Aviso **Para cumprir com os regulamentos de segurança, faça a montagem de switches em uma parede com o painel frontal virado para cima.**

¡Advertencia! **Para cumplir con las reglas de seguridad, instale los interruptores en una pared con el panel del frente hacia arriba.**

Varning! **För att uppfylla säkerhetsföreskrifter skall switcharna monteras på en vägg med frampanelen riktad uppåt.**

A biztonsági előírások betartása érdekében a kapcsolókat úgy szerelje a falra, hogy az előlapjuk felfelé nézzen.

Предупреждение В соответствии с положениями безопасности установите переключатели на стене передней панелью наружу.

警告 为符合安全规章，请将切换开关安装在墙上，前面板朝上。

警告 安全既定に準拠するために、フロントパネルを上向きにしてスイッチを壁にマウントします。

Related Documentation

These documents provide complete information about the Catalyst 3750 and3560, 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/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, and 2960 Switch System Message Guide*
- *Catalyst 3750 Switch Hardware Installation Guide*
- *Catalyst 3750 Getting Started Guide*
- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*

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

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

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide*
- *Catalyst 3560 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, and 2960 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 switches and are available on Cisco.com:

- *Catalyst 2960 Switch Software Configuration Guide*

- *Catalyst 2960 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, and 2960 Switch System Message 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 Switch*
- *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch*

For other information about related products, see these documents:

- Device manager online help (available on the switch)
- *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 documentationt:
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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.