# Release Notes for the Catalyst 3750, 3560, and 2960 Switches, Cisco IOS Release 12.2(50)SE and Later

**Revised October 21, 2010**

Cisco IOS Release 12.2(50)SE and later runs on all Catalyst 3750, 3560, and 2960 switches and on Cisco EtherSwitch service modules. Cisco IOS Release 12.2(50)SE2 includes only specific images for the Catalyst 2960 switches and Catalyst 3750 switches. See Table 4 on page 8.

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(50)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 3750, 3560, and 2960 switch documentation and of Cisco EtherSwitch service module documentation, see the "Related Documentation" section on page 78.

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

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

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

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 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 | Cisco IOS Release 12.2(18)SE |
| | 100BASE-FX MMF[6] | Cisco IOS Release 12.2(20)SE |
| SFP modules (Catalyst 2960) | 1000BASE-BX, -CWDM, -LX/LH, -SX, -ZX | Cisco IOS Release 12.2(25)FX |
| | 100BASE-BX, FX, -LX | |
| 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 | Supported on all software releases |
| | Cisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch) | Supported on all software releases |
| | Cisco Redundant Power System 2300 | Cisco IOS Release 12.2(35)SE and later |

1. 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

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

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.122-50.SE5.tar | Catalyst 3750 IP base image and device manager files.<br>This image has Layer 2+ and basic Layer 3 routing features.<br>This image also runs on the Cisco EtherSwitch service modules. |
| c3750-ipservices-tar.122-50.SE5.tar | Catalyst 3750 IP services image and device manager files.<br>This image has both Layer 2+ and full Layer 3 routing features.<br>This image also runs on the Cisco EtherSwitch service modules. |
| c3750-ipbasek9-tar.122-50.SE5.tar | Catalyst 3750 IP base cryptographic image and device manager files.<br>This image has the Kerberos, SSH[1], Layer 2+, and basic Layer 3 routing features.<br>This image also runs on the Cisco EtherSwitch service modules. |

*Table 4 Cisco IOS Software Image Files (continued)*

| Filename | Description |
|---|---|
| c3750-ipservicesk9-tar.122-50.SE5.tar | Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules. |
| c3560-ipbase-tar.122-50.SE5.tar | Catalyst 3560 IP base image file and device manager files. This image has Layer 2+ and basic Layer 3 routing features. |
| c3560-ipservices-tar.122-50.SE5.tar | Catalyst 3560 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features. |
| c3560-ipbasek9-tar.122-50.SE5.tar | Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features. |
| c3560-ipservicesk9-tar.122-50.SE5.tar | Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. |
| c2960-lanbase-tar.122-50.SE5.tar | Catalyst 2960 image file and device manager files. This image has Layer 2+ features. |
| c2960-lanbasek9-tar.122-50.SE5.tar | Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features. |
| c2960-lanlitek9-tar.122-50.SE5.tar | Catalyst 2960 LAN lite cryptographic image file and device manager files. |
| c2960-lanlite-tar.122-50.SE5.tar | Catalyst 2960 LAN lite image file and device manager files. |

1. SSH = Secure Shell

# Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility

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

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

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

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

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

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

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

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

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

# Archiving Software Images

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

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

http://www.cisco.com/en/US/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 (formerly known as the EMI) or IP base image (formerly known as the SMI) 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 (formerly known as the EMI) or IP base image (formerly known as the SMI) 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 37.

**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

These sections describe the new software features for this release:



### Catalyst 3750, 3560, and 2960 switches

These are the new features for the Catalyst 3750, 3560, and 2960 switches:

- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- IEEE 802.1x with open access to allow a host to access the network before being authenticated.
- IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch.
- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.
- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.
- Cisco EnergyWise manages the energy usage of power over Ethernet (PoE) entities.
- Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE).
- CPU utilization threshold trap monitors CPU utilization.
- Support for the Cisco IOS Configuration Engine, previously referred to as the Cisco IOS CNS agent.
- 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.
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Auto Smartports Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port.
- IP source guard restricts traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings (Catalyst 2960 switches).
- 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 (Catalyst 2960 switches).
- Support for these MIBs:
  - SCP attribute in the CONFIG_COPY MIB
  - CISCO-AUTH-FRAMEWORK-MIB

- CISCO-MAC-AUTH-BYPASS MIB
- LLDP MIB

## Catalyst 3750 and 3560 Switches

These are the new features for the Catalyst 3750 and 3560 switches:

- Intermediate System-to-Intermediate System (IS-IS) routing supports dynamic routing protocols for Connectionless Network Service (CLNS) networks.
- Support for Embedded Event Manager Version 2.4.
- Stack troubleshooting enhancements.
- These IPv6 features are now supported in the IP services and IP base software images:

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

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

## Catalyst 2960 switch

This feature was added to the Catalyst 2960 switch LAN Lite image:

Support for 802.1x authentication with restricted VLANs (also known as *authentication failed VLANs*) in all switch images.

# 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, 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 |
|---|---|---|
| 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 |
| 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 |

*Table 5 Catalyst 3750, 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 |
|---|---|---|
| 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 |
| 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 |

*Table 5 Catalyst 3750, 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 |
|---|---|---|
| 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 |
| 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 |

*Table 5 Catalyst 3750, 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 |
|---|---|---|
| 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 |
| Access SDM templates | 12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules |
| IPv6 ACLs | 12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules |
| IPv6 Multicast Listener Discovery (MLD) snooping | 12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules |
| QoS hierarchical policy maps on a port | 12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules |
| NAC Layer 2 IEEE 802.1x validation | 12.2(25)SED | 3750, 3560, 2960<br>Cisco EtherSwitch service modules |
| NAC Layer 2 IP validation | 12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules |
| IEEE 802.1x inaccessible authentication bypass. | 12.2(25)SED<br>12.2(25)SEE | 3750, 3560<br>Cisco EtherSwitch service module<br>2960 |
| IEEE 802.1x with restricted VLAN | 12.2(25)SED | 3750, 3560, 2960<br>Cisco EtherSwitch service modules |

*Table 5 Catalyst 3750, 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 |
|---|---|---|
| Budgeting power for devices connected to PoE ports | 12.2(25)SEC | 3750, 3560<br>Cisco EtherSwitch service modules |
| Multiple spanning-tree (MST) based on the IEEE 802.1s standard | 12.2(25)SEC<br>12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules<br>2960 |
| Unique device identifier (UDI) | 12.2(25)SEC<br>12.2(25)SED | 3750, 3560<br>Cisco EtherSwitch service modules<br>2960 |
| VRF Lite | 12.2(25)SEC | 3750, 3560<br>Cisco EtherSwitch service modules |
| IEEE 802.1x with wake-on-LAN | 12.2(25)SEC<br>12.2(25)SED | 3750, 3560<br>2960, Cisco EtherSwitch service modules |
| Nonstop forwarding (NSF) awareness | 12.2(25)SEC | 3750, 3560<br>Cisco EtherSwitch service modules |
| Configuration logging | 12.2(25)SEC<br>12.2(25)SED | 3750, 3560<br>2960, Cisco EtherSwitch service modules |
| Secure Copy Protocol | 12.2(25)SEC<br>12.2(25)SED | 3750, 3560<br>2960, Cisco EtherSwitch service modules |
| Cross-stack EtherChannel | 12.2(25)SEC | 3750<br>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<br>12.2(25)SED | 3750, 3560, 2960 |

*Table 5 Catalyst 3750, 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 |
|---|---|---|
| IGMP snooping querier | 12.2(25)SEA<br>12.2(25)FX | 3750, 3560, 2960 |
| Advanced IP services | 12.2(25)SEA | 3750, 3560 |
| Support for DSCP transparency | 12.2(25)SE<br>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<br>12.2(25)FX | 3750, 3560, 2960 |
| IEEE 802.1Q tunneling and Layer 2 protocol tunneling | 12.2(25)SE | 3750, 3560 |
| Layer 2 point-to-point tunneling and Layer 2 point-to-point tunneling bypass | 12.2(25)SE | 3750, 3560 |
| Support for SSL version 3.0 for secure HTTP communication (cryptographic images only) | 12.2(25)SE<br>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<br>12.2(25)FX | 3750, 3560, 2960 |
| Dynamic ARP inspection | 12.2(20)SE | 3750, 3560 |
| Flex Links | 12.2(20)SE<br>12.2(25)FX | 3750, 3560, 2960 |
| Software upgrade (device manager or Network Assistant only) | 12.2(20)SE<br>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<br>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<br>12.2(25)FX | 3750, 3560, 2960 |

*Table 5 Catalyst 3750, 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 |
|---|---|---|
| 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, page 21
- Device Manager Limitations, page 37


## Cisco IOS Limitations

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


- Configuration, page 22
- Ethernet, page 25
- Fallback Bridging, page 26
- HSRP, page 26
- IP, page 26
- IP Telephony, page 26
- MAC Addressing, page 27
- MAC Addressing, page 27
- Multicasting, page 27
- Power, page 30
- QoS, page 30
- Routing, page 31
- SPAN and RSPAN, page 31
- Stacking (Catalyst 3750 or Cisco EtherSwitch service module switch stack only), page 33
- Trunking, page 36
- VLAN, page 36

## 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 1, 2, 5, 6, 9, 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)

- 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)

## 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)

## 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)

- 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, 3560, and 2960 switches and for the Cisco EtherSwitch service modules:



## 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 master.

## 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.<br>• **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear.<br>• **enable**—Enable password, which is the default method of HTTP server user authentication, is used.<br>• **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

This section describes the open caveats with possible unexpected activity in this software release. Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Catalyst 3750, 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.

- CSCeh35595 (Cisco EtherSwitch service 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.

- 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.

- CSCsk96058 (Catalyst 3750 switches)

  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
  ```

- CSCsl02680 (Catalyst 3750 and 3560 switches)

  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.

- CSCso96778

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

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

- CSCsw68528

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

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

- CSCsw69006

  The **show mvr members** privileged EXEC command output does not include STATIC INACTIVE members. When a static port becomes ACTIVE, it appears in the output as expected.

  There is no workaround.

- CSCsw69015

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

  The workaround, if the groups are not displaying correctly, is to create the MVR VLAN *before* enabling MVR. The configuration then displays correctly.

- CSCsw96933 (Catalyst 3750 switches)

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

  There is no workaround.

- CSCsx25276 (Catalyst 3750 switches)

  When software is reloaded on a switch stack master that has port security enabled, the switch stack might crash.

  There is no workaround.

- 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.

- CSCsx51098 (Catalyst 3750 switches)

  If the switch stack software is reloaded while the ACS is unreachable, a port configured with a critical VLAN might become error disabled, and a message similar to the one shown below appears on the switch console:

  ```
  *Mar 3 01:10:13.423: %PM-4-ERR_DISABLE_VP: security-violation error detected on
  Fa8/0/7, vlan 3000.
  ```

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

- CSCsx56941 (Catalyst 3750 switches)

  After a PC connected to a switch in a stack is awakened by a Wake-on-LAN packet and authorized by MAC authentication bypass, a traceback message appears indicating a VLAN error.

  No workaround is necessary because the message does not affect switch functionality.

- CSCsx65958 (Catalyst 3750 switches)

  Following a stack reload, a port that is configured for single-host mode and is connected to a PC and an IP phone becomes error-disabled on the access VLAN.

  There is no workaround.

- CSCsx67722 (Catalyst 3750 switches)

  When EnergyWise is enabled and you reload member switches while leaving the stack master up, you might see a console traceback message similar to this:

  ```
  Feb 12 22:08:45: %INTERFACE_API-3-NOADDSUBBLOCK: The HWIDB subblock named ENERGYWISE
  was not added to GigabitEthernet4/0/49
  -Traceback= F943C8 F94B14 344E08 17D97E0 668798 A736B0 A73FB8 A743C8 BBAC28 BB16F8.
  ```

  This message is benign and does not cause any issues other than traceback.

  No workaround is required because the message does not affect functionality, but you can avoid console messages by reloading the master switch as well as the member switches.

- 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.

- 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.

- CSCsz43634 (Catalyst 2960 switches running the LAN-Lite image)

  Entering the **show archive** privileged EXEC command might cause the switch console to stop responding. This occurs if you have previously entered the **archive config** privileged EXEC command and that command failed due to either network problems or an unavailable TFTP server.

  The workaround is to power-cycle the switch.

- CSCsz88857 (Catalyst 3750 switches)

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

  These are possible workarounds:

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

- CSCta39338 (Catalyst 2960 and Catalyst 3560 switches)

  Entering the **udld enable** global configuration command is supposed to enable UniDirectional Link Detection (UDLD) only on fiber ports. You enter the **udld port** interface configuration command to enable UDLD on other port types. However, when you enter the **udld enable** global configuration command, UDLD is enabled by default on dual-media ports, even if a copper link is connected to an RJ-45 socket.

  The workaround is to manually disable UDLD on the port by entering the **no udld port** interface configuration command.

- CSCta57846

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

  The workaround is to enter the **logging file flash**:*filenam*

- CSCtb55994

  When EnergyWise Phase 1 is enabled on a switch that has unconnected interfaces, a memory leak might occur over several days. To verify this, use the **show process memory sorted holding | i energy wise** privileged EXEC command.

  The workaround is to disable EnergyWise on the switch.

- CSCtf35960 (Catalyst 3750 switches)

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

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

- CSCti79385

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

  There is no workaround.

# Resolved Caveats


- Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE5, page 44
- Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE4, page 44
- Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE3, page 51

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

- CSCte14603

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

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

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

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

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

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

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

- CSCsh59019

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

  There is no workaround.

- CSCsk85192

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

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

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

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

- CSCsx97605

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

  There is no workaround.

- CSCsy37362 (Catalyst 3750 switches)

  After you have entered the **snmp-server ifindex persist** global configuration command on a stacked Catalyst 3750 switch that is running Cisco IOS Release 12.2(50)SE, the switch fails and sends this error message:

  ```
  platform assert failure: hwidb->snmp_if_index == ifIndex:
  ../src-hulc/src-common/hpm_idbman.c: 1772: hpm_register_idb_with_snmp (Switch-4)
   -Traceback=
  ```

  There is no workaround. A Catalyst 3750 switch that is running Cisco IOS Release 12.2.(50)SE does not support the **snmp-server ifindex persist** global configuration command.

- CSCsy83366

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

  There is no workaround.

- CSCsy90265

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

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

- CSCsz66428

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

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

  Use one of these workarounds:

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

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

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

- CSCsz72234 (Catalyst 3750 and 3560 switches)

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

Use one of these workarounds:

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

- CSCta09189

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

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

  Use one of these workarounds:

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

- CSCta31785

  The TestPortAsicLoopback fails on the small form-factor pluggable (SFP) ports.

  There is no workaround. This does not affect how the switch runs.

- CSCta47293

  On a switch that supports Cisco Discovery Protocol (CDP) bypass, when a Cisco IP phone is connected to an 802.1x-enabled switch port that is in single host mode and that has a guest VLAN, a supplicant that does not send an Extensible Authentication Protocol over LAN (EAPOL)-start frame cannot be authorized.

  The workaround is to ensure that the supplicant sends an EAPoL-start frame.

- CSCta53893

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

  The workaround is to restart the switch.

- CSCta57846

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

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

- CSCta78502

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

  There is no workaround.

- CSCta87523

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

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

- CSCta97284 (Catalyst 2960 switches)

  A Catalyst 2960 switch that is running a LAN base software image of a release later than Cisco IOS Release 12.2(44)SE6 returns an `invalid CLI` message when you enter the **standby ip** interface configuration command and then the command fails.

  There is no workaround.

- CSCtb08426 (Catalyst 3750 switches)

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

  - The stack master has an active EtherChannel in Link Aggregation Control Protocol (LACP) mode.
  - The EtherChannel is cross-stacked.
  - There are two or more switches in each stack.

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

- CSCtb10158

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

  There is no workaround.

- CSCtb25230 (Catalyst 3750 switches)

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

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

- CSCtb56844

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

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

- CSCtb57486

  After you have entered the **authentication host-mode multi-auth** interface configuration command and have changed the access VLAN, MAC authentication bypass (MAB) does not work and authentication fails.

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

- CSCtb77378 (Catalyst 3750 and 3560 switches)

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

  The workaround is to remove the custom banner.

- CSCtb82729

  After you have entered the **switchport protected** interface configuration command on a switch that is running Cisco IOS Release 12.2(50)SE3 and that has Internet Group Management Protocol (IGMP) snooping globally enabled, multicast traffic is still forwarded between ports that should be protected.

  To workaround is to enter the **no ip igmp snooping** global configuration command.

- CSCtb83133 (Catalyst 2960 switches)

  On a Catalyst WS-C2960-48PST-L or WS-C2960-48PST-S switch, when you shut down an interface that is not connected to any device, another interface on the same switch that is connected to a device also goes down. The problem affects the Gi0/1 and Gi0/4 interfaces as a pair, and the Gi0/2 and Gi0/3 interfaces as a pair, and occurs when a 1000BaseSX SFP is installed in the interface that is connected to a device.

  The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that went down.

- CSCtb84303 (Catalyst 3750 switches)

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

  There is no workaround.

- CSCtb91572

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

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

- CSCtc39809

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

  There is no workaround.

- CSCtc43231

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

  There is no workaround.

- CSCtc57809

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

  – The physical interface is in a *no shut* state.

  – The MAC address is first dynamically learned and then changed to static.

  There is no workaround.

- CSCtc70571

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

  There is no workaround.

- CSCtc71798 (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.

  There is no workaround.

- CSCtc81879

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

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

- CSCtc90039

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

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

- CSCtd17296

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

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

- CSCtd30053

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

  There is no workaround.

- CSCtd31242

  An IP phone loses network connectivity under these conditions:

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

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

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

- CSCtd72456

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

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

- CSCtd72626

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

  There is no workaround.

- CSCtd73256

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

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

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

  When the switch fails, it sends this error message:

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

  There is no workaround.

- CSCte00827

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

  There is no workaround.

- CSCte67201

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

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

- CSCte81321

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

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

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

- CSCsl72774 (Catalyst 3750 and 3560 switches)

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

  **cef table consistency-check ipv4**

  **cef table consistency-check ipv6**

- CSCso57496

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

- CSCso90107 (Catalyst 3750 and 3560 switches)

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

- CSCsq24002

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

- CSCsq51052

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

- CSCsv32556 (Catalyst 3750 switches)

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

- CSCsw45277

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

- CSCsx36608 (Catalyst 3750 switches)

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

  – The stack members start at the same time because the stack reloaded or powered up.

  – The RADIUS server is down, the re-authentication timer expires, all the ports become unauthorized, and the RADIUS restarts.

  - All the ports on stack members are disabled and then re-enabled with the shutdown and no shutdown interface configuration commands at the same time.
  - The wake-on-LAN (WoL) feature is enabled and a large number of clients try to authenticate.

- CSCsx49718

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

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

- CSCsx70889

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsy07555

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsy15227

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

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

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

- CSCsy27389

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

- CSCsy48370

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

- CSCsy57970

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

- CSCsy66686

  The switch no longer reloads when the default port cost of service (CoS) value is updated on a port that has a policy map configured and CoS override enabled with the **mls qos cos override** privileged EXEC command.

- CSCsy71842

  The Layer 2 Protocol Tunneling (L2PT) drop-threshold protocol no longer continues to drop traffic after it is removed from the switch configuration.

- CSCsy72669

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

- CSCsy72726

  A switch running 12.2(50)SE or later no longer might unexpectedly restart when Auto Smart Ports is enabled and the switch is configured for SSH or the HTTP secure server is enabled by entering the **ip http secure-server** global configuration command.

- CSCsy79004 (Catalyst 3750 switches)

  The correct LED on a Catalyst 3750G-24TS switch now turns on when both Gigabit Ethernet 1/0/25, 1/0/26, 1/0/27, or 1/0/28 and the connected device has an established link.

- CSCsy91579

  A switch no longer randomly resets due to memory corruption.

- CSCsz12381

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

- CSCsz13490

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

- CSCsz14369

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

- CSCsz19002 (Catalyst 3750 and 3560 switches)

  IPv6 multicast packets are no longer forwarded between two isolated ports in the same private VLAN.

- CSCsz20321 (Catalyst 3750 and 3560 switches)

  BGP sessions with neighboring switches are no longer dropped when an inbound access-list is placed on the VLAN interface or on the routed physical interface across which the BGP sessions are established.

- CSCsz48211

  A data device can now receive an IP address through DHCP when

  - IEEE 802.1x authentication is configured on the switch port.
  - Multidomain authentication (MDA) is configured on the port.
  - An IP phone is not connected to the port, or the connected IP phone is not authenticated.
  - The device is in a guest or restricted VLAN.
  - DHCP snooping is configured on the VLAN.

- CSCsz77920

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

- CSCsz79293(Catalyst 3750 switches)

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

- CSCsz79652

  A memory leak no longer occurs when Cisco Network Assistant is polling the switch and the **ip http server** or **ip http-secure-server** global configuration command is enabled.

- CSCsz81762

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

- CSCsz89393 (Catalyst 3750 switches)

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

- CSCta32597

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

- CSCta36155

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

- CSCta56469

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

- CSCta67777

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

- CSCta78591 (Catalyst 3750V2 and 3560V2 PoE switches and Cisco Etherswitch service modules only)

  PoE switches now provide power to all legacy Cisco IP Phones.

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

- CSCsb46724

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

- CSCsr92741

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

- CSCsy24510

  The switch now accepts an encrypted secret password.

- CSCsy41470

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

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

- CSCso53157 (Catalyst 3750 switches)

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

- CSCsq26873

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

- CSCsq63926 (Catalyst 3750 and 3560 switches)

  The following message no longer appears when configuring an access list with large logical operation units (LOUs):

  ```
  *Mar 1 00:10:29.296 UTC: %ACLMGR-2-NOVMR: Cannot create VMR data structures for access
  list aclvlan42out
  ```

  Additionally tracebacks are no longer seen when applying some ACLs.

- CSCsq67398

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

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

- CSCsq89564

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

- CSCsr53843 (Catalyst 3750-48PS switches)

  When a stack member is connected to another switch through an uplink, the remote switch no longer prunes the member VLAN because there is no VTP join message from the stack member.

- CSCsr65689

  When loopback interfaces are configured, this error message no longer appears when a stack member is loading:

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

  No workaround is required. This does not affect switch functionality.

- CSCsr79279 (Catalyst 2960 switches)

  When disconnecting the Rx cable from a 1000BASE-X SFP module connected between a Catalyst 4000 Supervisor Engine IV and a Catalyst 2960 switch, the Catalyst 2960 switch does now correctly detects linkdown.

- CSCsr50766

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

- CSCsr64007

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

- CSCsr65689

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

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

- CSCsr77489 (Catalyst 2960 switches)

  An error message now appears when the Catalyst 2960 switch is in the VLAN Trunking Protocol (VTP) client mode or VTP server mode and you try to configure an interface with an access VLAN or trunk VLAN that is not part of the VTP domain. You can add the VLAN if the VLAN ID is less than 1001, and the number of VLANs configured in the switch is less than or equal to 64.

- CSCsr79279 (Catalyst 2960 switches)

  When the switch is connected to a Catalyst 4500 E-Series Supervisor Engine 6-E and the cable is disconnected from the Catalyst 4500 switch, it now detects the link-down condition.

- CSCsu06485 (Catalyst 3750 switches)

  A switch stack is connected to Switch 1 and Switch 1 in the spanning-tree topology:

  - Stack member 1 is connected to Switch 1 through the port 1/0/1.

    Switch 1 is the root bridge.

    Port 1/0/1 is in the forwarding state.

  - Stack member 3 is connected to Switch 2 through the port 3/0/1.

    Port 3/0/1 is in the blocking state.

  If you enter the **stack-mac persistent timer 5** global configuration command to set the time period to 5 minutes before the stack MAC address changes to that of the new stack master and then power off Switch 1, port 3/0/1 no longer takes 5 minutes to move from the blocking state to the forwarding state.

- CSCsu10065

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

- CSCsu57030 (Catalyst 3560 and 2960 switches)

  The *PMD Auto-Negotiation Advertised Capability* is now correct on the GigabitEthernet switch ports.

- CSCsu59214

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

- CSCsu88168

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

- CSCsu93869 (Catalyst 3750 switches)

  When the master switch in a Catalyst 3750 switch stack initiates an auto-copy process to automatically upgrade member switch images, the upgrade now succeeds when a member switch is in a version mismatch state.

- CSCsv04836

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

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

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsv16740

  After upgrading the switch software from IOS Release 12.2(25) SED1 to IOS Release 12.2(25) SEE4, you can now ping a switch virtual interface (SVI) from an isolated VLAN.

- CSCsv30429

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

- CSCsv64023

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

- CSCsv89005

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

- CSCsv91358

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

- CSCsv92967 (Catalyst 2960 switches)

  When a GLC-FE-100FX SFP is inserted in the Gigabit Ethernet port of a WS-C2960-24TC-L switch, the interface now correctly autonegotiates when it is defaulted.

- CSCsw17270 (Catalyst 3750 switches)

  You no longer see this message on a stack when spanning-tree loopguard is globally enabled: *%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port StackPort1 on VLAN0001.*

- CSCsw30249

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

- CSCsw45337

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

- CSCsw64692 (Catalyst 3750 switches)

  When a Catalyst 3750G switch with 48 ports is added to a stack where a Catalyst 3750G-12S is the stack master, auto- upgrade of the member switch software no longer fails.

- CSCsw65548

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

- CSCsw85180

  The switch now performs unequal-cost load balancing.

# Documentation Updates

This section provides these updates to the product documentation for the Catalyst 3750, 3560, and 2960 switches:



## Updates to the Catalyst 3750 and 3560 Switch Software Configuration Guides

- If the switch is running the IP base image, you can configure complete EIGRP routing. However, the configuration is not implemented because the IP base image supports only EIGRP stub routing, as described in the “Configuring IP Unicast Routing” chapter of the software configuration guide.

  After you have entered the **eigrp stub** router configuration command, only the **eigrp stub connected summary** command takes effect. Although the CLI help might show the **receive-only** and **static** keywords and the you can enter these keywords, the switch running the IP base image always behaves as if the **connected** and **summary** keywords were configured.

- In the “Multi-VRF CE Configuration Guidelines” section of the “Configuring IP Unicast Routing” chapter of the *Catalyst 3750 Switch Software Configuration Guide* and the *Catalyst 3560 Switch Software Configuration Guide*, this guideline is incorrect:

  If no VRFs are configured, 104 policies can be configured.

This is the correct guideline:

If no VRFs are configured, up to 105 policies can be configured.

- Although documented in the software configuration guide, VRF-Aware services for Unicast Reverse Path Forwarding (uRPF) is not supported.
- This information is added to the "Using IEEE 802.1x Authentication with Per-User ACLs" section of "Configuring IEEE 802.1x Port-Based Authentication" chapter of the software configuration guide:

  Per-user ACLs are supported only in single-host mode.
- In the "Configuration Guidelines" section of the "Configuring Flex Links and the MAC Address-Table Move Update Feature" chapter, this guideline is added:

  You can configure up to 16 backup links.
- This information is added to the "Using Route Maps to Redistribute Routing Information" section in the "Configuring IP Unicast Routing" chapter of the software configuration guide:

**Note** A route map with no **set** route-map configuration commands is sent to the CPU, which causes high CPU utilization.

# Updates to the Catalyst 2960 Switch Software Configuration Guides

This section was added to the "Configuring IEEE 802.1x Port-Based Authentication" chapter:

## Using 802.1x Authentication with Per-User ACLs

You can enable per-user access control lists (ACLs) to provide different levels of network access and service to an 802.1x-authenticated user. When the RADIUS server authenticates a user connected to an 802.1x port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1x port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

You can configure router ACLs and input port ACLs on the same switch. However, a port ACL takes precedence over a router ACL. If you apply input port ACL to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL applied to the VLAN interface. Incoming packets received on the port to which a port ACL is applied are filtered by the port ACL. Incoming routed packets received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router ACL. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS server.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are `inacl#<n>` for the ingress direction and `outacl#<n>` for the egress direction. MAC ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports. For more information, see Chapter 35, "Configuring Network Security with ACLs."

Use only the extended ACL syntax style to define the per-user configuration stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if you use the Filter-Id attribute, it can point to a standard ACL.

You can use the Filter-Id attribute to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by *.in* for ingress filtering or *.out* for egress filtering. If the RADIUS server does not allow the *.in* or *.out* syntax, the access list is applied to the outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

Only one 802.1x-authenticated user is supported on a port. If multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

For examples of vendor-specific attributes, see the "Configuring the Switch to Use Vendor-Specific RADIUS Attributes" section on page 10-29. For more information about configuring ACLs, see Chapter 35, "Configuring Network Security with ACLs."

To configure per-user ACLs, you need to perform these tasks:

- Enable AAA authentication.
- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication.
- Configure the user profile and VSAs on the RADIUS server.
- Configure the 802.1x port for single-host mode.

For more configuration information, see the "Authentication Manager" section on page 11-7.

# Updates for the Catalyst 3750V2 and 3560V2 Switches

## Catalyst 3750 and 3560 Software Configuration Guides

- In the "Availability and Redundancy Features" section of the "Overview" chapter:

  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.
- In the "Hardware Loopback" section of the "Configuring Switch Stacks" chapter:

  On Catalyst 3750V2 members, the *Loopback HW* value is always *N/A*.
- In the "Configuring Interface Characteristics" chapter:

### 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.<br>The keywords have these meanings:<br>• *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.<br>• **name**—Set the name of the RPS 2300, and enter one of these options:<br>– *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.<br>– **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.<br>The keywords have these meanings:<br>• *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.<br>• **port** *rps-port-id*—Specify the RPS 2300 port. The range is from 1 to 6.<br>• **mode**—Set the mode of the RPS 2300 port:<br>– **active**—The RPS 2300 can provide the power to a switch when the switch internal power supply cannot.<br>– **standby**—The RPS 2300 is not providing power to a switch.<br>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.<br>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, 2970, or 2960 switches—RPS 2300 or Cisco RPS 675 Redundant Power System, also referred to as the RPS 675.

## Catalyst 3750 and 3560 Command References

The **power rps** user EXEC command is added, and the **show env** user EXEC command is modified.

### power rps

Use the **power rps** user EXEC command on the switch stack or on a standalone switch to configure and manage the Cisco Redundant Power System 2300, also referred to as the RPS 2300, connected to the switch stack or a standalone switch.

**power rps** *switch-number* {**name** {*string* | **serialnumber**} | **port** *rps-port-id* {**mode** {**active** | **standby**}{**priority** *priority*}

**Note** The **power rps** command is supported only on the Catalyst 3750V2 and 3560V2 switches.

**Syntax Description**

| | |
|---|---|
| *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.<br>This parameter is available only on Catalyst 3750V2 switches. |
| **name** {*string* \| **serialnumber**} | Set the RPS name:<br>• Enter a *string* to 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.<br>• Enter the **serialnumber** keyword to configure the switch to use the RPS serial number as the name. |
| **port** *rps-port-id* | Specify the RPS port. The range is from 1 to 6. |
| **mode** {**active** \| **standby**} | Set the RPS port mode:<br>• **active**—The RPS can provide power to a switch when the switch internal power supply cannot.<br>• **standby**—The RPS is not providing power to a switch. |
| **priority** *priority* | Set the priority of the RPS port. The range is from 1 to 6.<br>• A value of 1 assigns highest priority to a port and its connected device.<br>• A value of 6 assigns lowest priority to a port and its connected device. |

**Defaults**

The RPS name is not configured.

The RPS ports are in **active** mode.

The RPS port priority is 6.

**Command Modes**

User EXEC

**Command History**

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

**Usage Guidelines**

The **power rps** command applies only to an RPS 2300 connected to a Catalyst 3560V2 switch, a Catalyst 3750V2 standalone switch, or a switch stack.

When configuring an RPS 2300 connected to a stack member, you must specify the member before entering the name or serial number of the RPS.

In a standalone switch, the name applies to the connected redundant power system. In a switch stack, the name applies to the redundant power system ports connected to the specified switch. For example, if a stack of nine switches is connected to three redundant power systems and you enter the **power rps 1 name "abc"** command, the name of the redundant power system connected to switch 1 is *abc*, and the names of the other redundant power systems are not changed.

If you do not want the RPS to provide power to a switch connected to the specified RPS port but do not want to disconnect the RPS cable between the switch and the redundant power system, use the **power rps** *switch-number* **port** *rps-port-id* **mode standby** 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.

The **no power rps** user EXEC command is not supported.

- To return to the default name setting (no name is configured), use the **power rps** *switch-number* **port** *rps-port-id* **name** global configuration command with no space between the quotation marks.
- To return to the default RPS port mode, use the **power rps** *switch-number* **port** *rps-port-id* **active** command.
- To return to the default RPS port priority, use the **power rps** *switch-number* **port** *rps-port-id* **priority** command.

## Examples

This example shows how to configure the name of the RPS 2300 that is connected to a switch stack as a *string*:

```
Switch> power rps 2 name RPS_Accounting
```

This example shows how to configure the name of the RPS 2300 that is connected to a switch as the serial number:

```
Switch> power rps name serialnumber
```

This example shows how to configure the mode of RPS port 1 as standby on a switch:

```
Switch> power rps port 1 mode standby
```

This example shows how to configure the priority of RPS port 3 with a priority value of 4 on a switch:

```
Switch> power rps 1 port 3 priority 4
```

You can verify your settings by entering the **show env power** or the **show env rps** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show env power** | Displays the status of the power supplies for a switch or switch stack. |
| **show env rps** | Displays the status of the redundant power systems connected to a switch or switch stack. |

## show env

Use the **show env** user EXEC command to show fan, temperature, redundant power system (RPS) availability, and power information for the switch (standalone, stack master, or stack member). Use with the **stack** keyword to show all information for the stack or for a specified switch in the stack.

**show env** {**all** | **fan** | **power** | **rps** [**all** | **detail** | **switch** [*switch-number*]] | **stack** [*switch-number*] | **temperature** [**status**]} [ | {**begin** | **exclude** | **include**} *expression*]

**Syntax Description**

| | |
|---|---|
| **all** | Display both fan and temperature environmental status. |
| **fan** | Display the switch fan status. |
| **power** | Display the switch power status. |
| **rps** | Display any connected redundant power system.<br>• Catalyst 3750-E or 3560-E switch—Only the Cisco Redundant Power System 2300, also referred to as the RPS 2300.<br>• Catalyst 3750V2 or 3560V2 switch—Only the RPS 2300.<br>• Catalyst 3750, 3560, 2970, or 2960 switches—RPS 2300 or Cisco RPS 675 Redundant Power System, also referred to as the RPS 675. |
| **rps all** | (Optional) Display all the redundant power systems that are connected to the standalone switch or the switch stack.<br>These keywords are available only on Catalyst 3750V2 and 3560V2 switches. |
| **rps detail** | (Optional) Display the details about the redundant power systems that are connected to the switch or the switch stack.<br>These keywords are available only on Catalyst 3750V2 and 3560V2 switches. |
| **rps switch** [*switch-number*] | (Optional) Display the redundant power systems that are connected to each switch in the stack or to the specified switch. For *switch-number*, the range is 1 to 9, depending on the switch member numbers in the stack.<br>These keywords are available only on Catalyst 3750V2 switches. |
| **stack** [*switch-number*] | Display all environmental status for each switch in the stack or for the specified switch. The range is 1 to 9, depending on the switch member numbers in the stack. |
| **temperature** | Display the switch temperature status. |
| **status** | (Optional) Display the switch internal temperature (not the external temperature) and the threshold values. This keyword is available only on the Catalyst 3750G-48TS, 3750G-48PS, 3750G-24TS-1U, and 3750G-24PS and on the Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches. |
| **\| 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* | Expression in the output to use as a reference point. |

**Command Modes**

User EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.1(11)AX | This command was introduced. |
| 12.2(20)SE3 | The **temperature status** keyword was added. |
| 12.2(50)SE | The **rps** [**all** \| **detail** \| **switch** [*switch-number*]] keywords were added. |

## Usage Guidelines

Use the **session** privileged EXEC command for information about a specific switch other than the master.

Use the **show env stack** [*switch-number*] command to display information about any switch in the stack from any member switch.

Though visible on all switches, the **show env temperature status** command is valid only for the Catalyst 3750G-48TS, 3750G-48PS, 3750G-24TS-1U, and 3750G-24PS and for the Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches. If you enter this command on these switches, the command output shows the switch temperature states and the threshold levels. If you enter the command on other than these switches, the output field shows *Not Applicable*.

On a Catalyst 3750G-48PS or 3750G-24PS or on a Catalyst 3560G-48PS or 3560G-24PS switch, you can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command on this switch, the command output is the same as the **show env temperature status** command output.

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

For more information about the threshold levels, see the software configuration guide for this release.

## Examples

This is an example of output from the **show env all** command entered from the master switch or a standalone switch:

```
Switch> show env all
FAN is OK
TEMPERATURE is OK
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 56 Degree Celsius
Red Threshold    : 66 Degree Celsius
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
 1  Built-in                                         Good

SW  Status          RPS Name          RPS Serial#  RPS Port#
--  -------------   ----------------  -----------  ---------
```

This is an example of output from the **show env fan** command:

```
Switch> show env fan
FAN is OK
```

This is an example of output from the **show env rps** command on a stack master:

```
Switch> show env rps
SW  Status          RPS Name          RPS Serial#  RPS Port#
--  -------------   ----------------  -----------  ---------
3   Active          CiscoRPS          CAT1050VGF3  3

RPS Name: CiscoRPS
  State: Active
  PID: PWR-RPS2300
  Serial#: CAT1050VGF3
  Fan: Good
  Temperature: Green

  RPS Power Supply A: Present
    PID             : C3K-PWR-750WAC
    Serial#         : DTH1050M04S
```

```
    System Power    : Good
    PoE Power       : Good
    Watts           : 300/420 (System/PoE)

  RPS Power Supply B: Present
    PID             : C3K-PWR-750WAC
    Serial#         : DTH1050M03H
    System Power    : Good
    PoE Power       : Good
    Watts           : 300/420 (System/PoE)

DCOut  State   Connected  Priority  BackingUp  WillBackup  Portname         SW#
-----  ------- ---------  --------  ---------  ----------  ---------------- ---
    1  Active  Yes               6  Yes        Yes         <>                 -
    2  Active  Yes               6  Yes        Yes         <>                 -
    3  Active  Yes               3  No         Yes         Switch             3
    4  Active  No                1  No         Yes         <>                 -
    5  Active  No                6  No         No          <>                 -
    6  Active  No                6  No         No          <>                 -
```

This is an example of output from the **show env rps all** command on a stack master:

```
Switch> show env rps all
SWITCH 1:
RPS:
    RPS is active
    Fan:           Good
    Temperature:   Green

DC port legends:
Y   = Yes                       :  N   = No
Act = Active                    :  Sby = Standby
OK  = Power Supply is good      :  NP  = Power Supply is not present or bad
BU  = RPS actively backing up   :  NB  = RPS not actively backing up
12v/PoE  12v/PoE   RPS
Port  State  Prio   Status   Backup   Avail  PortName         Switch Name
----  -----  ----   ------   ------   -----  ---------------  ---------------
 1     Act     1    OK/OK    NB/NB      Y    <>               <remote>
 2     Act     4    OK/NP    NB/NB      Y    <>               <remote>
 3     Act     1    OK/OK    NB/NB      Y    <>               Switch
 4     Act     1    OK/OK    NB/NB      Y    Switch           <remote>
 5     Act     2    OK/OK    NB/NB      Y    <>               <remote>
 6     Act     6    OK/OK    NB/NB      Y    <>               <remote>

<output truncated>
```

This is an example of output from the **show env stack** command:

```
Switch> show env stack
SWITCH: 1
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 2
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

```
SWITCH: 4
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 5
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
SWITCH: 6
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This example shows how to display information about stack member 3 from the master switch:

```
Switch> show env stack 3
SWITCH: 3
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This example shows how to display the temperature value, state, and the threshold values. Table 6 describes the temperature states in the command output.

```
Switch> show env temperature status
Temperature Value:28 Degree Celsius
Temperature State:GREEN
Yellow Threshold :70 Degree Celsius
Red Threshold    :75 Degree Celsius
```

***Table 6 States in the show env temperature status Command Output***

| State | Description |
|---|---|
| Green | The switch temperature is in the *normal* operating range. |
| Yellow | The temperature is in the *warning* range. You should check the external temperature around the switch. |
| Red | The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range. |

# Updates to the Command Reference Guides

# debug authentication

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

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

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

## Syntax Description

| | |
|---|---|
| **acct** | (Optional) Display authentication manager accounting information. |
| **all** | (Optional) Display all authentication manager debug messages. |
| **auth_fail_vlan** | (Optional) Display authentication manager errors for the restricted VLAN. |
| **auth_policy** | (Optional) Display authentication policy messages. |
| **autocfg** | (Optional) Display autoconfiguration authentication manager debug messages. |
| **critical** | (Optional) Display the inaccessible authentication bypass messages.<br>**Note** The inaccessible authentication bypass feature is also referred to as critical authentication or the authentication, authorization, and accounting (AAA) fail policy. |
| **dhcp** | (Optional) Display authentication manager debug messages on DHCP dynamic address-enable interfaces. |
| **errors** | (Optional) Display all authentication manager error debug messages. |
| **events** | (Optional) Display all authentication manager event debug messages, including registry and miscellaneous events. |
| **feature** | (Optional) Display authentication manager feature debug messages |
| **guest_vlan** | (Optional) Display guest VLAN authentication manager messages. |
| **mab_pm** | (Optional) Display MAC authentication manager bypass authentication debug messages. |
| **mda** | (Optional) Display multidomain authentication manager debug messages. |
| **multi_auth** | (Optional) Display multi-authentication manager debug authentication messages. |
| **switch_pm** | (Optional) Display switch port manager messages. |
| **switch_sync** | (Optional) Display synchronization messages between the switch, the authentication server, and the connected devices. |
| **sync** | (Optional) Display operational synchronization authentication manager debug messages. |
| **vlan_assign** | (Optional) Display the VLAN-assignment debug messages. |
| **voice** | (Optional) Display the voice-VLAN debug messages. |
| **webauth** | (Optional) Display web authentication manager debug messages. |

## Defaults

Authentication debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

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

**Usage Guidelines**

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

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

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

**Related Commands**

| Command | Description |
|---|---|
| **authentication control-direction** | Configures the port mode as unidirectional or bidirectional. |
| **authentication event** | Sets the action for specific authentication events. |
| **authentication fallback** | Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. |
| **authentication host-mode** | Sets the authorization manager mode on a port. |
| **authentication open** | Enables or disables open access on a port. |
| **authentication order** | Sets the order of authentication methods used on a port. |
| **authentication periodic** | Enables or disables reauthentication on a port. |
| **authentication port-control** | Enables manual control of the port authorization state. |
| **authentication priority** | Adds an authentication method to the port-priority list. |
| **authentication violation** | Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port. |
| **show authentication** | Displays information about authentication manager events on the switch. |

# Updates to the 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** `ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]`

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

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

**Error Message** `ACLMGR-3-INVALIDPARAM: Invalid [chars] [int] encountered`

**Explanation** The access control list (ACL) manager has encountered an invalid parameter value. [chars] is the parameter name, and [int] is the parameter value.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section.

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

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

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

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

**Recommended Action** No action is required.

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

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

**Recommended Action** No action is required.

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

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

**Recommended Action** No action is required.

**Error Message** `PLATFORM_HCEF-3-ADJ: [chars]`

**Explanation** This message appears when an unsupported feature is configured on a switch running Cisco IOS Release 12.2(25)SE. [chars] is the error message.

**Recommended Action** Determine if a generic routing encapsulation (GRE) tunnel or the **ip cef accounting** global configuration command are configured. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnels are supported. If the GRE tunnel is configured, remove the tunnel, or upgrade the switch software to a Cisco IOS release when the GRE feature is needed. If the **ip cef accounting** command is configured, remove it by using the **no ip cef accounting** global configuration command.

**Note** Cisco IOS Release12.2(25)SEB2 does not support the **ip cef accounting** command.

**Error Message** `PLATFORM_IPv6_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

**Explanation** A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ipv6 unicast retry route** privileged EXEC command lists the failed prefixes.

**Recommended Action** No action is required.

**Error Message** `PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

**Explanation** A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

**Recommended Action** No action is required.

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

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

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the system message guides.

**Error Message** `SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans`

**Explanation** The interface has been added to all VLANs. [chars] is the added interface.

**Recommended Action** No action is required.

**Error Message** `SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans`

**Explanation** The interface has been deleted from all VLANs. [chars] is the deleted interface.

**Recommended Action** No action is required.

**Error Message** `SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].`

**Explanation** The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

**Recommended Action** No action is required.

These messages were added to the Catalyst 3750 and 3560 system message guides:

**Error Message** `VQPCLIENT-2-TOOMANY: Interface [chars] shutdown by active host limit.`

**Explanation** The system has shut down the specified interface because too many hosts have requested access to that interface. [chars] is the interface name.

**Recommended Action** To enable the interface, remove the excess hosts, and enter the **no shutdown** interface configuration command.

**Error Message** `VQPCLIENT-3-VLANNAME: Invalid VLAN [chars] in response.`

**Explanation** The VLAN membership policy server (VMPS) has specified a VLAN name that is unknown to the switch. [chars] is the VLAN name.

**Recommended Action** Ensure that the VLAN exists on the switch. Verify the VMPS configuration by entering the **show vmps** privileged EXEC command.

**Error Message** `PLATFORM_WCCP-4-SDM_MISMATCH: WCCP requires sdm template routing`

**Explanation** The switch database management (SDM) routing template is not specified on the switch.

**Recommended Action** Specify the SDM routing template to be used. Enter the **sdm prefer routing** global configuration command, and then enter the **reload** privileged EXEC command to reload the switch.

**Error Message** `WCCP-5-CACHEFOUND: Web Cache [IP_address] acquired.`

**Explanation** The switch has acquired the specified web cache. [IP_address] is the web cache IP address.

**Recommended Action** No action is required.

**Error Message** `WCCP-1-CACHELOST: Web Cache [IP_address] lost.`

**Explanation** The switch has lost contact with the specified web cache. [IP_address] is the web cache IP address.

**Recommended Action** Verify the operation of the web cache by entering the **show ip wccp web-cache** privileged EXEC command.

## Changed System Messages

The error explanation and action has changed for these system messages:

**Error Message** `EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.`

**Explanation** The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

**Recommended Action** Ensure that the other ports in the bundle have the same configuration.

**Error Message** `ILPOWER-3-CONTROLLER_PORT_ERR:Controller port error, Interface Fa0/7:Power given, but link is not up.`

**Note** This message applies only to the Catalyst 3750 and 3560 switches.

**Explanation** The inline-power-controller reported an error on an interface.

**Recommended Action** Enter the **shutdown** and **no shutdown** interface configuration commands on the affected interfaces. Upgrade to Cisco IOS Release12.1(14)EA1 or later, which provides an electrostatic discharge (ESD) recovery mechanism.

## Deleted System Messages

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

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

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

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

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

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

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

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

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

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

# Updates to the Catalyst 3750, 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 7 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<br>(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<br>(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 8 Catalyst 2960-48PST-S, Catalyst 2960-24PC-S, and Catalyst 2960-24LC-S Specifications***

| **Power Requirements** | |
|---|---|
| AC input voltage | 100 to 240 VAC (autoranging)<br>8 to 4 A, 50 to 60 Hz (Catalyst 2960-24PC-S)<br>3 to 1.5 A, 50 to 60 Hz (Catalyst 2960-24LC-S)<br>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)<br>12 V⎓@ 8.3 A, –48 V⎓@ 2.7 A (Catalyst 2960-24LC-S)<br>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)<br>51 W, 174 BTUs per hour (Catalyst 2960-24LC-S)<br>483 W, 1647 BTUs per hour (Catalyst 2960-48PST-S) |
| Power rating | 0.470 KVA (Catalyst 2960-24PC-S)<br>0.175 KVA (Catalyst 2960-24LC-S)<br>0.5 KVA (Catalyst 2960-48PST-S) |

*Table 8 Catalyst 2960-48PST-S, Catalyst 2960-24PC-S, and Catalyst 2960-24LC-S Specifications (continued)*

| | |
|---|---|
| **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)<br>10 lb (4.54 kg) (Catalyst 2960-24LC-S)<br>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*.

# 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.** |
| **Figyelem** | **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, 3560, 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 W*ireless *LAN Controller Command Reference, Release 4.0*

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide*
- *Catalyst 3560 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, 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 documentation, at:

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

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

---