



Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(37)SE and Later

Revised August 8, 2007

Cisco IOS Releases 12.2(37)SE and later run on all Catalyst 3750, 3560, 2970, and 2960 switches and on Cisco EtherSwitch service modules.

The Catalyst 3750 switches and the Cisco EtherSwitch service modules support stacking through Cisco StackWise technology. The Catalyst 3560, 2970, 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(37)SE and 12.2(37)SE1 and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 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 7.

For the complete list of Catalyst 3750, 3560, 2970, and 2960 switch documentation and of Cisco EtherSwitch service module documentation, see the “[Related Documentation](#)” section on page 52.

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 8-week 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

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

This information is in the release notes:

- “System Requirements” section on page 2
- “Upgrading the Switch Software” section on page 6
- “Installation Notes” section on page 12
- “New Features” section on page 12
- “Minimum Cisco IOS Release for Major Features” section on page 13
- “Limitations and Restrictions” section on page 17
- “Important Notes” section on page 30
- “Open Caveats” section on page 32
- “Resolved Caveats” section on page 38
- “Documentation Updates” section on page 42
- “Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page 54

System Requirements

The system requirements are described in these sections:

- “Hardware Supported” section on page 2
- “Device Manager System Requirements” section on page 5
- “Cluster Compatibility” section on page 6
- “CNA Compatibility” section on page 6

Hardware Supported

Table 1 lists the hardware supported on this release.

Table 1 Catalyst 3750, 3560, 2970, 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

Table 1 *Catalyst 3750, 3560, 2970, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware (continued)*

Switch	Description	Supported by Minimum Cisco IOS Release
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
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 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(37)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 2970G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 2970G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 2960-8TC	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

Table 1 Catalyst 3750, 3560, 2970, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960G-8TC	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 2960-24TC	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(25)FX
Catalyst 2960-48TC	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(25)FX
Catalyst 2960-24TT	24 10/100BASE-T Ethernet ports and 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-48TT	48 10/100BASE-T Ethernet ports 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-24TC	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	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

Table 1 Catalyst 3750, 3560, 2970, and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
SFP modules (Catalyst 3750, 3560, and 2970)	1000BASE-CWDM ⁵ , -LX, SX, -T, -ZX 100BASE-FX MMF ⁶	Cisco IOS Release 12.2(18)SE Cisco IOS Release 12.2(20)SE
SFP modules (Catalyst 2960)	1000BASE-BX, -CWDM, -LX/LH, -SX, -ZX 100BASE-BX, FX, -LX	Cisco IOS Release 12.2(25)FX
XENPAK modules ⁷	XENPAK-10-GB-ER, XENPAK-10-GB-LR, and XENPAK-10-GB-SR	Cisco IOS Release 12.2(18)SE
Redundant power systems	Cisco RPS 675 Redundant Power System Cisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch) Cisco Redundant Power System 2300	Supported on all software releases Supported on all software releases Cisco IOS Release 12.2(35)SE and later (not supported on Catalyst 2970 switches)

- PoE = Power over Ethernet
- SFP = small form-factor pluggable
- 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.
- Cisco EtherSwitch service module
- CWDM = coarse wavelength-division multiplexer
- MMF = multimode fiber
- 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](#)” section on page 5
- “[Software Requirements](#)” section on page 6

Hardware Requirements

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

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II ¹	64 MB ²	256	1024 x 768	Small

- We recommend Intel Pentium 4.
- We recommend 256-MB DRAM.

Software Requirements

Table 3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.



Note

The device manager does not require a plug-in.

Table 3 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer ¹	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

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(37)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” section on page 7
- “Deciding Which Files to Use” section on page 7
- “Upgrading a Switch by Using the Device Manager or Network Assistant” section on page 10
- “Upgrading a Switch by Using the CLI” section on page 10
- “Recovering from a Software Failure” section on page 12

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.



Note

For Catalyst 3750 and 3560 switches and the Cisco EtherSwitch service modules, although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base image [formerly known as the SMI] or IP services image [formerly known as the EMI]) and does not change if you upgrade the software image.

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

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

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

Cisco IOS Release 12.2(25)SEB and later refers to the Catalyst 2970 image as the *LAN base* image.

[Table 4](#) lists the different file-naming conventions before and after Cisco IOS Release 12.2(25)SEB.

Table 4 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

Table 4 Cisco IOS Image File Naming Convention (continued)

Cisco IOS 12.2(25)SEA and earlier	Cisco IOS 12.2(25)SEB and later
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
c2970-i612-mz	c2970-lanbase-mz
c2970-i6k9112-mz	c2970-lanbasek9-mz

1. SMI = standard multilayer image
2. EMI = enhanced multilayer image

Table 5 lists the filenames for this software release.



Note

For IPv6 capability on the Catalyst 3750 or 3560 switch or on the Cisco EtherSwitch service modules, you must order the advanced IP services image upgrade from Cisco.

Table 5 Cisco IOS Software Image Files

Filename	Description
c3750-ipbase-tar.122-37.SE1.tar	Catalyst 3750 IP base image and device manager files. This image has Layer 2+ and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipservices-tar.122-37.SE1.tar	Catalyst 3750 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipbasek9-tar.122-37.SE1.tar	Catalyst 3750 IP base cryptographic image and device manager files. This image has the Kerberos, SSH ¹ , Layer 2+, and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipservicesk9-tar.122-37.SE1.tar	Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules.
c3750-advipservicesk9-tar.122-37.SE1.tar	Catalyst 3750 advanced IP services image, cryptographic file, and device manager files. This image has all the IP services image (formerly known as the EMI) features and the capability for unicast routing of IPv6 packets. This image also runs on the Cisco EtherSwitch service modules.
c3560-ipbase-tar.122-37.SE1.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.122-37.SE1.tar	Catalyst 3560 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features.

Table 5 Cisco IOS Software Image Files (continued)

Filename	Description
c3560-ipbasek9-tar.122-37.SE1.tar	Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3560-ipservicesk9-tar.122-37.SE1.tar	Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3560-advipservicesk9-tar.122-37.SE1.tar	Catalyst 3560 advanced IP services image, cryptographic file, and device manager files. This image has all the IP services image (formerly known as the EMI) features and the capability for unicast routing of IPv6 packets.
c2970-lanbase.122-37.SE1.tar	Catalyst 2970 image file and device manager files. This image has Layer 2+ features.
c2970-lanbasek9-tar.122-37.SE1.tar	Catalyst 2970 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanbase-tar.122-37.SE1.tar	Catalyst 2960 image file and device manager files. This image has Layer 2+ features.
c2960-lanbasek9-tar.122-37.SE1.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.

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. If the image versions are not compatible, the wireless LAN controller switch could stop functioning.

[Table 6](#) is the compatibility matrix for Catalyst 3750 and wireless controller.

Table 6 Catalyst 3750G Wireless LAN Controller Switch Software Compatibility

Switch Software Release	Compatible Controller Software Release
Cisco IOS Release 12.2(25)FZ	Cisco Software Release 4.0.x.0
Cisco IOS Release 12.2(35)SE	Cisco Software Release 4.0.x.0
Cisco IOS Release 12.2(37)SE	Cisco Software Release 4.1.x.0

For information about this controller software release, see the [Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Point, Release 4.0.x.0](#). For controller software upgrade procedure, see the [Cisco Wireless LAN Controller Configuration Guide Release 4.0](#).

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 5 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 image for a Catalyst 2970 switch, click **Catalyst 2970 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2970 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 or a Catalyst 2970 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.122-37.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 30](#).

**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

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

- [“New Hardware Features” section on page 12](#)
- [“New Software Features” section on page 12](#)

New Hardware Features

There are no new hardware features for this release. For a list of all supported hardware, see the [“Hardware Supported” section on page 2](#).

New Software Features

These are the new software features for this release:

- IP phone detection enhancement to detect and recognize a Cisco IP phone
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones

- DHCP Snooping Statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form (Catalyst 3750, 3560, and 2960 switches)
- PIM stub routing to reduce resource usage by moving routed traffic closer to the end user (Catalyst 3750 and 3560 switches)
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port (Catalyst 3750 and 3560 switches)
- VLAN aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port
- Support for auto rendezvous point (auto-RP) for multicast, which uses IP multicast to automate the distribution of group-to-RP mappings to all Cisco routers and multilayer switches in a PIM network (Catalyst 3750 and 3560 switches)
- VLAN Flex Links load balancing to configure a Flex Links pair to allow both ports to forward traffic for some VLANs (mutually exclusive) (Catalyst 3750, 3560, 2960)
- Web Cache Communication Protocol (WCCP) for redirecting traffic to wide-area application engines, for enabling content requests to be fulfilled locally, and for localizing web-traffic patterns in the network (Catalyst 3750 and 3560 switches; requires the IP services image)
- SNMP support for the Port Error Disable MIB
- Support for the Time Domain Reflectometry MIB

Minimum Cisco IOS Release for Major Features

Table 7 lists the minimum software release required to support the major features of the Catalyst 3750, 3560, 2970, and 2960 switches and the Cisco EtherSwitch service modules.

Table 7 Catalyst 3750, 3560, 2970, 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
IP phone detection enhancement	12.2(37)SE	3750, 3560, 2970, 2960
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE	3750, 3560, 2970, 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, 2970, 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 7 *Catalyst 3750, 3560, 2970, 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, 2970, 2960
EIGRP stub routing in the IP base image	12.2(25)SEE	3750, 3560
/31 bit mask support for unicast traffic	12.2(25)SEE	3750, 3560
Access SDM templates	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 ACLs	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 Multicast Listener Discovery (MLD) snooping	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
QoS hierarchical policy maps on a port	12.2(25)SED	3750, 3560, and 2970 Cisco EtherSwitch service modules
NAC Layer 2 IEEE 802.1x validation	12.2(25)SED	3750, 3560, 2970, and 2960 Cisco EtherSwitch service modules
NAC Layer 2 IP validation	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x inaccessible authentication bypass.	12.2(25)SED 12.2(25)SEE	3750, 3560 Cisco EtherSwitch service module 2960 and 2970
IEEE 802.1x with restricted VLAN	12.2(25)SED	3750, 3560, 2970, and 2960 Cisco EtherSwitch service modules
Budgeting power for devices connected to PoE ports	12.2(25)SEC	3750 and 3560 Cisco EtherSwitch service modules

Table 7 *Catalyst 3750, 3560, 2970, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEC	3750, 3560, and 2970 Cisco EtherSwitch service modules
	12.2(25)SED	2960
Unique device identifier (UDI)	12.2(25)SEC	3750, 3560, and 2970 Cisco EtherSwitch service modules
	12.2(25)SED	2960
VRF Lite	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x with wake-on-LAN	12.2(25)SEC	3750, 3560, 2970
	12.2(25)SED	2960, Cisco EtherSwitch service modules
Nonstop forwarding (NSF) awareness	12.2(25)SEC	3750 and 3560 Cisco EtherSwitch service modules
Configuration logging	12.2(25)SEC	3750, 3560, 2970
	12.2(25)SED	2960, Cisco EtherSwitch service modules
Secure Copy Protocol	12.2(25)SEC	3750, 3560, 2970
	12.2(25)SED	2960, Cisco EtherSwitch service modules
Cross-stack EtherChannel	12.2(25)SEC	3750 Cisco EtherSwitch service modules
Support for configuring private-VLAN ports on interfaces that are configured for dynamic ARP inspection (IP base image [formerly known as the SMI] only)	12.2(25)SEB	3750 and 3560
Support for IP source guard on private VLANs (IP base image [formerly known as the SMI] only)	12.2(25)SEB	3750 and 3560
Support for configuring an IEEE 802.1x restricted VLAN	12.2(25)SED	3750, 3560, 2970, and 2960
IGMP leave timer	12.2(25)SEB	3750, 3560, and 2970
	12.2(25)SED	2960
IGMP snooping querier	12.2(25)SEA	3750, 3560, 2970, and 2960
	12.2(25)FX	
Advanced IP services	12.2(25)SEA	3750, 3560
Support for DSCP transparency	12.2(25)SE	3750, 3560, 2970, and 2960
	12.2(25)FX	
Support for VLAN-based QoS ¹ and hierarchical policy maps on SVIs ²	12.2(25)SE	3750, 3560, 2970
Device manager	12.2(25)SE	3750, 3560, 2970, and 2960
	12.2(25)FX	

Table 7 *Catalyst 3750, 3560, 2970, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
IEEE 802.1Q 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 12.2(25)FX	3750, 3560, 2970, and 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 and 3560
Support for IP source guard on private VLANs (IP services image [formerly known as the EMI] only)	12.2(25)SE	3750 and 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 and 3560
IEEE 802.1x accounting and MIBs (IEEE 8021-PAE-MIB and CISCO-PAE-MIB)	12.2(20)SE 12.2(25)FX	3750, 3560, 2970, and 2960
Dynamic ARP inspection (IP services image [formerly known as the EMI] only)	12.2(20)SE	3750 and 3560
Flex Links	12.2(20)SE 12.2(25)FX	3750, 3560, 2970, and 2960
Software upgrade (device manager or Network Assistant only)	12.2(20)SE 12.2(25)FX	3750, 3560, 2970, and 2960
IP source guard (IP services image [formerly known as the EMI] only)	12.2(20)SE	3750, 3560
Private VLAN (IP services image [formerly known as the EMI] only)	12.2(20)SE	3750, 3560
SFP module diagnostic management interface	12.2(20)SE 12.2(25)FX	3750, 3560, 2970, and 2960
Switch stack offline configuration	12.2(20)SE	3750
Stack-ring activity statistics	12.2(20)SE	3750
Smartports macros	12.2(18)SE 12.2(25)FX	3750, 3560, 2970, and 2960
Generic online diagnostics (GOLD)	12.2(25)SEE	3750
Flex Links Preemptive Switchover	12.2(25)SEE	3750, 3560, 2970, and 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” section on page 17](#)
- [“Device Manager Limitations” section on page 29](#)

Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3750, 3560, 2970, and 2960 switches and the Cisco EtherSwitch service modules:

- [“Configuration” section on page 17](#)
- [“Ethernet” section on page 19](#)
- [“Fallback Bridging” section on page 20](#)
- [“HSRP” section on page 20](#)
- [“IP” section on page 21](#)
- [“IP Telephony” section on page 21](#)
- [“MAC Addressing” section on page 21](#)
- [“Management” section on page 21](#)
- [“Multicasting” section on page 22](#)
- [“QoS” section on page 24](#)
- [“Routing” section on page 24](#)
- [“SPAN and RSPAN” section on page 25](#)
- [“Stacking \(Catalyst 3750 or Cisco EtherSwitch service module switch stack only\)” section on page 27](#)
- [“Trunking” section on page 29](#)
- [“VLAN” section on page 29](#)

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, 3560, or 2970 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, 3560, or 2970 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)

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

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
 - Ports 3, 4, 7, 8, 11, 12, 15, 16, 19, and 20 of the Catalyst 2970G-24T and 2970G-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:

- 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)
- 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)
- 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)

Management

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

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)

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

There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

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

There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
 - You disable IP multicast routing or re-enable it globally on an interface.
 - A switch mroute table temporarily runs out of resources and recovers later.

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

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

Use one of these workarounds:

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

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

Power

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):

- 2970G-24T
- 2970G-24TS
- 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):

- 2970G-24T
 - 2970G-24TS
 - 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)

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)

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, 2970, and 2960 switches and for the Cisco EtherSwitch service modules:

- “Switch Stack Notes” section on page 30
- “Cisco IOS Notes” section on page 30
- “Device Manager Notes” section on page 31

Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- The Catalyst 3560 and 2970 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 or a 2970 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, 3560, and 2970 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.

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:

- Choose **Tools > Internet Options**.
 - Click **Settings** in the “Temporary Internet files” area.
 - From the Settings window, choose **Automatically**.
 - Click **OK**.
 - Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip http authentication {aaa enable local}	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> aaa—Enable the authentication, authorization, and accounting feature. You must enter the aaa new-model interface configuration command for the aaa keyword to appear. enable—Enable password, which is the default method of HTTP server user authentication, is used. local—Local user database, as defined on the Cisco router or access server, is used.

	Command	Purpose
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, `http://10.1.126.45:184` where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {enable local tacacs}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> enable—Enable password, which is the default method of HTTP server user authentication, is used. local—Local user database, as defined on the Cisco router or access server, is used. tacacs—TACACS server is used.
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, `www.cisco.com:84`), you must enter `http://` as the URL prefix. Otherwise, you cannot launch the device manager.

Open Caveats

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, 2970, and 2960 switches and to Cisco EtherSwitch service modules:

- CSCef84975 (Cisco EtherSwitch service modules)

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.

- 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.

- CSCsb85001

If traffic is passing through VMPS ports and you perform a **shut** operation, a dynamic VLAN is not assigned and a VLAN with a null ID appears.

The workaround is to clear the MAC address table. This forces the VMPS server to correctly reassign the VLAN.

- CSCsc96474

The switch might display tracebacks similar to these examples when a large number of IEEE 802.1x supplicants try to repeatedly log in and log out.

Examples:

```
Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
```

```
Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
invalid for the current ate 'auth_restart': dot1x_auth Fa4
```

```
Jan 3 19:06:13 L3A3 310: -Traceback= B37A84 18DAB0 3046F4 302C80 303228 8F2B64 8E912C
Jan 3 20:41:44 L3A3 315: .Jan 3 20:51:26.249: %SM-4-BADEVENT: Event 'eapSuccess' is
invalid for the current state 'auth_restart': dot1x_auth Fa9
```

```
Jan 3 20:41:44 L3A3 316: -Traceback= B37A84 18DAB0 304648 302C80 303228 8F2B64 8E912C
```

There is no workaround.

- CSCsd03580

When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, some interface level configuration commands, including the **dot1x timeout** and **dot1x mac-auth-bypass commands**, become unavailable.

The workaround is to enable the **dot1x system-auth-control** global configuration command before attempting to configure interface level IEEE 802.1x parameters.

on command to the configuration and re-establishes communication with the RADIUS server.

- CSCse06827 (Catalyst 3750 switches)

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

The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.

- CSCse51203 (Catalyst 3750 and 3560 switches)

When the dynamic ARP inspection trust setting is removed from a large number of ports across multiple members of a stack, a `%PLATFORM_RPC-3-MSG_THROTTLED` message might appear.

The workaround is to remove the trust settings on a small number of ports one switch at a time. If the problem still occurs, continue to reduce the number of ports.

- CSCse75508 (Catalyst 3750 switches)

When cross-stack UplinkFast (CSUF) is configured on a switch and one of the member ports is flapping, packets transmitted from an EtherChannel port might be duplicated.

There is no workaround.

- CSCse88619 (Catalyst 3750 switches)

The error message `%HPSECURE-6-ADDR_REMOVED` might appear in a switch stack under these conditions:

- Port security is enabled on at least one port.
- Some secure addresses exist in the switch state.
- A new member joins a switch stack.

There is no workaround.

- CSCsf32504 (Catalyst 3750 switches)

When there are more than five switches in a stack or when four or more switches join a stack, there might be a long delay between the time the `Ready` prompt appears and a switch that is starting up begins carrying traffic. This delay can last several minutes.

There is no workaround. However, this condition only causes a delay during switch startup, and no data is lost.

- CSCsg21537 (Catalyst 3750 switches)

When MAC addresses are learned on an Etherchannel port, the addresses are incorrectly deleted from the MAC address table even when the MAC address table aging timeout value is configured to be longer than the ARP timeout value. This causes intermittent unicast packet flooding in the network.

The MAC address is automatically relearned after the ARP refresh. The workaround is to enter the **ping ip address** privileged EXEC command from the switch to the next hop router to avoid the intermittent flooding.

- CSCsg62919 (Catalyst 3750 switches)

Clearing secure addresses by entering the **clear port-security** global configuration command in a stack member might cause traffic to be dropped from the switch. Some secure addresses learned on the stack master might not be learned on a stack member. Packets with a secure source address might also be dropped.

These are the workarounds. You only need to do one of these:

- Enter the **clear port-security** global configuration command to stop the traffic.
- Enter the **shut** and **no shut** interface configuration commands on the port where the traffic is being dropped.

- CSCsg79506

During repeated reauthentication of supplicants on an IEEE 802.1x-enabled switch, if the RADIUS server is repeatedly going out of service and then coming back up, the available switch memory might deplete over time, eventually causing the switch to shut down.

There is no work-around, except to ensure that the RADIUS server is stable.

- CSCsg81185 (Catalyst 3750 and 3560 switches)

When a device is attached to a multidomain authentication (MDA)- enabled port that has IEEE 802.1x guest VLAN configured but not MAC authentication bypass (MAB), if the switch gets its MAC address from that port, the device is authenticated in the guest VLAN but appears as an IEEE 802.1x-authenticated device.

The workaround is to enable MAB by entering the **dot1x mac-auth-bypass** interface configuration command, or enter the **dot1x timeout tx-period 1** to set the IEEE 802.1x timeout period to 1 second.

- CSCsg81334

If IEEE 802.1x critical authentication is not enabled and the RADIUS authentication server is temporarily unavailable during a reauthentication, when the RADIUS server comes back up, MAC authentication bypass (MAB) does not authenticate a previously authenticated client.

The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command on the port connected to the client. An alternative, to prevent the problem from occurring, is to enable critical authentication by entering the **dot1x critical {eapol | recovery delay milliseconds}** global configuration command.

- CSCsh12472 (Catalyst 3750 and 3560 switches)

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-channell1
(ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
4CEB50 859DF4 A7BF28 A98260 882658 879A58
```

There is no workaround.

- CSCsh37209 (Catalyst 3750 switches)

When a stack master switchover event occurs, the backup interface might have traffic loss for up to 4 seconds.

This can occur under these conditions:

- One of the two interfaces in the backup interface pair is an EtherChannel.
- The EtherChannel interface is in a forwarding or active state.
- The member interface for the EtherChannel is not present on the next stack master switch.
- A failure occurs on the switch stack master.

There is no workaround

- CSCsi01526 (Catalyst 3750 and 3560 switches)

Traceback messages appear if you enter the **no switchport** interface configuration command to change a Layer 2 interface that belongs to a port channel to a routed port.

There is no workaround.

- CSCsi16162 (Catalyst 3750 and 3560 switches)

When you enter an all 0s route with an all 1s mask in the routing table and the next hop is entered as an interface, a traceback message appears.

The workaround is to use an IP address as the next hop instead of an interface.

- CSCsi26392

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.

- CSCsi26444

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

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

You can use one of these workarounds:

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

- CSCsi27545

When port security is configured on a PVLAN interface, the dynamic MAC address is not removed from the interface.

You can use one of these workarounds:

- Remove the dynamic MAC address by using the **clear mac-address-table dynamic** privileged EXEC command.
- Enter the **shut** and **no shut** interface configuration commands to reset the interface.
- Disable and then re-enable the VLANs.

- CSCsi52707

When setting an interface to its default configuration by using the **default** command, or when clearing the 802.1X mac-auth-bypass configuration from a port that was never authenticated, this message might appear:

```
01:18:09: %SM-4-STOPPED: Event 'mabAbort' ignored because the state machine is
stopped: dot1x_auth_mab -Traceback= 1D2368 3C1BA8 3C1D40 3C16A8 9EF8D8 9E6CC4
```

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

- CSCsi52914 (Catalyst 3750 switches)

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

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

The workaround is to reboot the switch stack.

- CSCsi65551 (Catalyst 3750 switches)

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

There is no workaround.

- CSCsi69447 (Catalyst 3750 switches)

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.

- CSCsi75246

An address learned as a supplicant that is aged out by port security aging is never relearned by port security under any of these conditions:

- IEEE 802.1x authentication, port security, and port security aging are enabled on a port.
- An address is cleared by port security.
- You enter the **clear port security** privileged EXEC command.

The workaround is to use the **dot1x timeout** interface configuration command instead of the port security aging timer as the reauthentication timer for IEEE 802.

- CSCsi06399 (Catalyst 3750 switches)

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

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

- CSCsi57905 (Catalyst 3750 switches)

During switch configuration, an error message similar to this might appear:

```
00:07:17: platform assert failure: 0: ../src-hulc/src-common/hspan.c: 817:
hspan_get_sasq_session 00:07:17: -Traceback= 503148 9218EC 922C8C 922040 923AB0
9242CC 927DD0 9186B0 918BA8 914714 CCADF0 CE73F0 9EF8D8 9E6CC4
```

This message might appear under these conditions:

- You configure two SPAN source sessions and an RSPAN destination session on a standalone switch and then modify the session RPSPAN VLAN.
- You configure an RSPAN destination session and two source sessions on the switch and a stack master failover occurs.

There is no workaround necessary. This message does not affect switch functionality.

Resolved Caveats

These are the caveats that have been resolved in these releases:

- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(37\)SE1”](#)
- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.2\(37\)SE”](#)

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(37)SE1

Unless otherwise noted, these resolved caveats apply to the Catalyst 3750, 3560, 2970, and 2960 switches and the Cisco EtherSwitch service modules.

- CSCsc19259

The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device’s filesystem, including the device’s saved configuration. This configuration file may include passwords or other sensitive information.

The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>.

- CSCsj13619

The SCP (Secure Copy Protocol) support is now correctly included in the image. The **show file systems** and **copy** privileged EXEC commands now correctly show **scp** as an option.

- CSCsj19641

The switch no longer drops ARP packets destined to MAC addresses that are close to the MAC address block of the switch.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(37)SE

Unless otherwise noted, these resolved caveats apply to the Catalyst 3750, 3560, 2970, and 2960 switches and the Cisco EtherSwitch service modules.

- CSCsb12598

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsb40304

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

**Note**

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsc30733

This error message no longer appears during authentication when a method list is used and one of the methods in the method list is removed:

```
AAA-3-BADMETHODERROR:Cannot process authentication method 218959117
```

- CSCsd85587

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

**Note**

Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

- CSCsd92405

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCse97398 (Catalyst 3750 and 3560 switches)

The **reload** privileged EXEC command now works correctly. In previous releases, the command sometimes did not cause the to reload when it was entered after these events occurred:

- A configuration file that contained crypto key generate rsa was copied to the switch running configuration by using the SNMP copy configuration command.
- An SNMP set was performed.
- c. The **reload** privileged EXEC command was entered.

- CSCse01557 (Catalyst 3750 switches)

The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` no longer appears for a switch stack under these conditions:

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

- CSCsg18176 (Catalyst 3750 and 3560 switches)

When dynamic ARP inspection is enabled and IP validation is disabled, the switch no longer drops ARP requests that have a source address of 0.0.0.0.

- CSCsg30295
When you configure an IP address on a switch virtual interface (SVI) with DHCP and enable DHCP snooping on the SVI VLAN, the switch SVI now obtains an IP address.
- CSCsg70039 (Catalyst 3750 and 3560 switches)
When both an authorized data domain and an authorized voice domain are present on a port, and you change the VLAN configuration on the port to equal the assigned VLAN, a traceback error no longer appears.
- CSCsg94672 (Catalyst 3750 and 3560 switches)
An IEEE 802.1x port configured for Multi-Domain Authentication now allows access to the guest VLAN if an IEEE 802.1x supplicant has previously been authenticated and was then logged off.
- CSCsg95349 (3750 and 3560 only)
When multicast routing and IGMP snooping are enabled, a member switch that receives join messages at a high rate can now correctly forward multicast traffic to all the multicast groups after a reload.
- CSCsh70266 (Catalyst 2960 switches)
The far-end fault setting now works correctly on a GLC-FE-100FX SFP module that is installed in a Catalyst 2960 switch.
- CSCsh92834
When trunk ports are participating in a Flex Link configuration, entering a **shutdown** or **no shutdown** interface configuration command on the port no longer causes the switch to reload.
- CSCsh92844
Online insertion and removal (OIR) of an SFP module no longer causes error-disabled ports to change to Up or Standby states, resulting in lost data.
- CSCsi00879
When IGMP snooping is enabled, multicast traffic no longer is dropped after a port channel interface link flaps.
- CSCsi23359 (Catalyst 3750 switches)
A Catalyst 3750 switch no longer unexpectedly reloads when a ping is sent to one of the switch multicast addresses.
- CSCsi30888
The switch no longer halts when configuring link-state tracking with EtherChannel downstream ports or when booting up a switch already configured with link-state tracking with EtherChannel downstream ports.

Documentation Updates

This section provides these updates to the product documentation for the Catalyst 3750, 3560, 2970, and 2960 switches:

- [“Updates to the Catalyst 3750, 3560, and 2960 Software Configuration Guide” section on page 43](#)
- [Updates to the Catalyst 3750 and 3560 Switch Command References, page 43](#)
- [Updates to the Catalyst 3750 Getting Started Guide, page 48](#)
- [Updates to the Catalyst 3750, 3560, 2970, and 2960 Hardware Installation Guide, page 47](#)

- [Updates to the Catalyst 2970 Software Configuration Guide, page 51](#)
- [Updates for the Regulatory Compliance and Safety Information, page 51](#)

Updates to the Catalyst 3750, 3560, and 2960 Software Configuration Guide

This section was added to the “Configuring IEEE 802.1x” chapter:

Web Authentication with Automatic MAC Check

You can use web authentication with automatic MAC check to authenticate a client that does not support IEEE 802.1x or web browser functionality. This allows end hosts, such as printers, to automatically authenticate by using the MAC address without any additional required configuration.

Web authentication with automatic MAC check only works in web authentication standalone mode. You cannot use this if web authentication is configured as a fallback to IEEE 802.1x authentication.

The MAC address of the device must be configured in the Access Control Server (ACS) for the automatic MAC check to succeed. The automatic MAC check allows managed devices, such as printers, to skip web authentication.



Note

The interoperability of web authentication (with automatic MAC check) and IEEE 802.1x MAC authentication configured on different ports of the same switch is not supported.

Updates to the Catalyst 3750 and 3560 Switch Command References

Commands for dynamic Address Resolution Protocol (ARP) inspection were revised in Cisco IOS Release 12.2(37)SE. These changes have not yet been incorporated into the command reference for this release.

- [ip arp inspection validate, page 43](#)
- [ip arp inspection vlan logging, page 45](#)
- [show ip arp inspection, page 47](#)

ip arp inspection validate

Use the **ip arp inspection validate** global configuration command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to return to the default settings.

```
ip arp inspection validate {[src-mac] [dst-mac] [ip [allow zeros] ]}
```

```
no ip arp inspection validate [src-mac] [dst-mac] [ip [allow zeros] ]
```

Syntax Description

src-mac	Compare the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
dst-mac	Compare the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
ip	Compare the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are compared in all ARP requests and responses. Target IP addresses are checked only in ARP responses.
allow-zeros	Modifies the IP validation test so that ARPs with a sender address of 0.0.0.0 (ARP probes) are not denied.

Defaults

No checks are performed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(20)SE	This command was introduced.
12.2(37)SE	The allow-zero keyword was added.

Usage Guidelines

You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables **src-mac** and **dst-mac** validations, and a second command enables IP validation only, the **src-mac** and **dst-mac** validations are disabled as a result of the second command.

The **allow-zeros** keyword interacts with ARP access control lists (ACLs) in this way:

- If you configure an ARP ACL to deny ARP probes, they are dropped even if the **allow-zero** keyword is specified.
- If you configure an ARP ACL that specifically permits ARP probes and configure the **ip arp inspection validate ip** command, ARP probes are dropped unless you enter the **allow-zeros** keyword.

The **no** form of the command disables only the specified checks. If none of the options are enabled, all checks are disabled.

Examples

This example show how to enable source MAC validation:

```
Switch(config)# ip arp inspection validate src-mac
```

You can verify your setting by entering the **show ip arp inspection vlan** *vlan-range* privileged EXEC command.

Related Commands	Command	Description
	show inventory vlan <i>vlan-range</i>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

ip arp inspection vlan logging

Use the **ip arp inspection vlan logging** global configuration command to control the type of packets that are logged per VLAN. Use the **no** form of this command to disable this logging control.

```
ip arp inspection vlan vlan-range logging {acl-match {matchlog | none} | dhcp-bindings {all | none | permit} | arp-probe}
```

```
no ip arp inspection vlan vlan-range logging {acl-match | dhcp-bindings | arp-probe}
```

Syntax Description		
	<i>vlan-range</i>	Specify the VLANs configured for logging. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
	acl-match { matchlog none }	Specify that the logging of packets is based on access control list (ACL) matches. The keywords have these meanings: <ul style="list-style-type: none"> matchlog—Log packets based on the logging configuration specified in the access control entries (ACE). If you specify the matchlog keyword in this command and the log keyword in the permit or deny ARP access-list configuration command, Address Resolution Protocol (ARP) packets permitted or denied by the ACL are logged. none—Do not log packets that match ACLs.
	dhcp-bindings { permit all none }	Specify the logging of packets is based on Dynamic Host Configuration Protocol (DHCP) binding matches. The keywords have these meanings: <ul style="list-style-type: none"> all—Log all packets that match DHCP bindings. none—Do not log packets that match DHCP bindings. permit—Log DHCP-binding permitted packets.
	arp-probe	Specify logging of packets permitted specifically because they are ARP probes.

Defaults

All denied or all dropped packets are logged. ARP probe packets are not logged.

Command Modes Global configuration

Command History

Release	Modification
12.2(20)SE	This command was introduced.
12.2(37)SE	The arp-probe keyword was added.

Usage Guidelines

The term *logged* means that the entry is placed into the log buffer and that a system message is generated.

The **acl-match** and **dhcp-bindings** keywords merge with each other; that is, when you configure an ACL match, the DHCP bindings configuration is not disabled. Use the **no** form of the command to reset the logging criteria to their defaults. If neither option is specified, all types of logging are reset to log when ARP packets are denied. These are the options:

- **acl-match**—Logging on ACL matches is reset to log on deny.
- **dhcp-bindings**—Logging on DHCP binding matches is reset to log on deny.

If neither the **acl-match** or the **dhcp-bindings** keywords are specified, all denied packets are logged.

The implicit deny at the end of an ACL does not include the **log** keyword. This means that when you use the **static** keyword in the **ip arp inspection filter vlan** global configuration command, the ACL overrides the DHCP bindings. Some denied packets might not be logged unless you explicitly specify the **deny ip any mac any log** ACE at the end of the ARP ACL.

Examples

This example shows how to configure ARP inspection on VLAN 1 to log packets that match the **permit** commands in the ACL:

```
Switch(config)# arp access-list test1
Switch(config-arp-nacl)# permit request ip any mac any log
Switch(config-arp-nacl)# permit response ip any any mac any any log
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
```

You can verify your settings by entering the **show ip arp inspection vlan *vlan-range*** privileged EXEC command.

Related Commands

Command	Description
arp access-list	Defines an ARP ACL.
clear ip arp inspection log	Clears the dynamic ARP inspection log buffer.
ip arp inspection log-buffer	Configures the dynamic ARP inspection logging buffer.
show inventory log	Displays the configuration and contents of the dynamic ARP inspection log buffer.
show inventory vlan <i>vlan-range</i>	Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN.

show ip arp inspection

The output of this command has changed to include the ARP probe information.

This is an example of output from the **show ip arp inspection** command

```
Switch# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Enabled

Vlan      Configuration      Operation      ACL Match      Static ACL
-----
1         Enabled             Active        deny-all      No

Vlan      ACL Logging      DHCP Logging      Probe Logging
-----
1         Acl-Match        All             Permit

Vlan      Forwarded      Dropped      DHCP Drops      ACL Drops
-----
1         0                0            0                0

Vlan      DHCP Permits      ACL Permits      Probe Permits      Source MAC Failures
-----
1         0                0            0                0

Vlan      Dest MAC Failures      IP Validation Failures      Invalid Protocol Data
-----
1         0                0                0                0
```

Updates to the Catalyst 3750, 3560, 2970, 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 to the Catalyst 3750 Getting Started Guide

The Express Setup configuration windows were updated in the getting started guide. This is the complete procedure:

Running Express Setup

When you first set up the switch, you should use Express Setup to enter the initial IP information. This enables the switch to connect to local routers and the Internet. You can then access the switch through the IP address for further configuration.

To run Express Setup:

- | | | |
|---------------|--|--|
| Step 1 | <p>Make sure that nothing is connected to the switch.</p> <p>During Express Setup, the switch acts as a DHCP server. If your PC has a static IP address, change your PC settings before you begin to temporarily use DHCP.</p> | |
| Step 2 | <p>Power the switch by connecting the supplied AC power cord to the switch power connector and to a grounded AC outlet.</p> | |
| Step 3 | <p>When the switch powers on, it begins the power-on self-test (POST). During POST, the LEDs blink while tests verify that the switch functions properly.</p> <p>Wait for the switch to complete POST, which can take several minutes.</p> | |
| Step 4 | <p>Verify that POST has completed by confirming that the SYST LED remains green. If the switch fails POST, the SYST LED turns amber.</p> <p>POST errors are usually fatal. Contact your Cisco technical support representative if your switch fails POST.</p> | |
| Step 5 | <p>Press and hold the Mode button for 3 seconds. When all of the LEDs left of the Mode button turn green, release the Mode button.</p> <p>If the LEDs left of the Mode button begin to blink after you press the button, release it. Blinking LEDs mean that the switch has already been configured and cannot go into Express Setup mode. For more information, see the “Resetting the Switch” section.</p> |  |
| Step 6 | <p>Verify that the switch is in Express Setup mode by confirming that all LEDs left of the Mode button are green. (On some models, the RPS and PoE LEDs remain off.)</p> | |
| Step 7 | <p>Connect a Category 5 Ethernet cable to any 10/100 or 10/100/1000 Ethernet port on the switch front panel.</p> <p>Connect the other end of the cable to the Ethernet port on your PC.</p> |  |

Step 8 Verify that the switch and PC Ethernet ports LEDs are green.
Wait 30 seconds.

Step 9 Start a web browser on your PC.
Enter the IP address 10.0.0.1 in the web browser, and press **Enter**.



The Express Setup page appears. If it does not appear, see the “In Case of Difficulty” section for help.



Step 10 Enter this information in the **Network Settings** fields:

- In the **Management Interface (VLAN ID)** field, the default is 1. Enter a new VLAN ID only if you want to change the management interface through which you manage the switch. The VLAN ID range is 1 to 1001.
- In the **IP Address** field, enter the IP address of the switch. In the **IP Subnet Mask** field, click the drop-down arrow, and select an **IP Subnet Mask**.
- In the **Default Gateway** field, enter the IP address for the default gateway (router).
- Enter your password in the **Switch Password** field. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Switch Password** field, enter your password again.

Step 11 (Optional) You can enter the **Optional Settings** information now or enter it later by using the device manager interface:

- In the **Host Name** field, enter a name for the switch. The host name is limited to 31 characters. Embedded spaces are not allowed.
- Enter the date, time, and time zone information in the **System Date**, **System Time**, and **Time Zone** fields. Click **Enable** to enable daylight saving time.

-
- Step 12** (Optional) Click the **Advanced Settings** tab on the Express Setup window, and enter the advanced settings now or enter them later by using the device manager interface.



-
- Step 13** (Optional) Enter this information in the **Advanced Setting** fields:
- In the **Telnet Access** field, click **Enable** if you are going to use Telnet to manage the switch by using the command-line interface (CLI). If you enable Telnet access, you must enter a Telnet password.
 - In the **Telnet Password** field, enter a password. The Telnet password can be from 1 to 25 alphanumeric characters, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Telnet Password** field, re-enter the Telnet password.
 - In the **SNMP** field, click **Enable** to enable Simple Network Management Protocol (SNMP). Enable SNMP only if you plan to manage switches by using CiscoWorks 2000 or another SNMP-based network-management system.
 - If you enable SNMP, you must enter a community string in the **SNMP Read Community** field, the **SNMP Write Community** field, or both. SNMP community strings authenticate access to MIB objects. Embedded spaces are not allowed in SNMP community strings. When you set the SNMP read community, you can access SNMP information, but you cannot modify it. When you set the SNMP write community, you can both access and modify SNMP information.
 - In the **System Contact** and **System Location** fields, enter a contact name and the wiring closet, floor, or building where the switch is located.

-
- Step 14** (Optional) You can enable Internet Protocol version 6 (IPv6) on the switch. From the **Advanced Settings** tab, check the **Enable IPv6** check box.



Note Enabling IPv6 restarts the switch when you complete Express Setup.

-
- Step 15** To complete Express Setup, click **Submit** from the **Basic Settings** or the **Advanced Settings** tab to save your settings, or click **Cancel** to clear your settings.

When you click **Submit**, the switch is configured and exits Express Setup mode. The PC displays a warning message and tries to connect with the new switch IP address. If you configured the switch with an IP address that is in a different subnet from the PC, connectivity between the PC and the switch is lost.

-
- Step 16** Disconnect the switch from the PC, and install the switch in your production network. See the “Managing the Switch” section for information about configuring and managing the switch.

If you need to rerun Express Setup, see the “Resetting the Switch” section.

Updates to the Catalyst 2970 Software Configuration Guide

Addition to the “Supported MIBs” Chapter

The CISCO-CABLE-DIAG-MIB was added to the “Supported MIBs” chapter.

The CISCO-ERR-DISABLE-MIB was added to the “Supported MIBs” chapter.

Updates for the Regulatory Compliance and Safety Information

Documentation Update to the *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*

This warning replaces Statement 100C:

Statement 370—Attaching the Cisco RPS to the RPS Receptacle



Warning

Attach only the following Cisco RPS model to the RPS receptacle:

PWR-RPS2300, PWR675-AC-RPS-N1= Statement 370

Waarschuwing

Sluit alleen het volgende Cisco RPS-model aan op de RPS-ontvanger:

PWR-RPS2300, PWR675-AC-RPS-N1=

Varoitus

Kiinnitä vain seuraava Cisco RPS malli RPS-astiaan:

PWR-RPS2300, PWR675-AC-RPS-N1=

Attention

Raccordez le modèle Cisco RPS suivant uniquement au connecteur RPS :

PWR-RPS2300, PWR675-AC-RPS-N1=

Warnung

Schließen Sie ausschließlich das folgende Cisco RPS-Modell an die Anschlussstelle für die redundante Stromversorgung an.

PWR-RPS2300, PWR675-AC-RPS-N1=

Avvertenza

Collegare soltanto il seguente modello Cisco RPS alla presa RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

Advarsel

Du må bare koble følgende Cisco RPS-modell til RPS-mottakeren:

PWR-RPS2300, PWR675-AC-RPS-N1=

Aviso

Introduza apenas o seguinte modelo RPS da Cisco no receptáculo RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

¡Advertencia!

Acople únicamente el siguiente modelo Cisco RPS al receptáculo RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

Varning! Bifoga endast följande Cisco RPS-modell till RPS-behållaren:
PWR-RPS2300, PWR675-AC-RPS-N1=

PWR-RPS2300, PWR675-AC-RPS-N1=

PWR-RPS2300, PWR675-AC-RPS-N1=

PWR-RPS2300, PWR675-AC-RPS-N1=

PWR-RPS2300, PWR675-AC-RPS-N1=

Related Documentation

These documents provide complete information about the Catalyst 3750, 3560, 2970, 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/hw/switches/ps5206/tsd_products_support_series_home.html
- http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the URL referenced in the [Obtaining Documentation, Obtaining Support, and Security Guidelines](#) section.

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

- *Catalyst 3750 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Getting Started Guide* (order number DOC-7816663=)
- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide* (order number DOC-7817540=)
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch* (order number DOC-7816664)

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* (order number DOC-7817540=)

- *Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0*
- *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*
- *Cisco Wireless LAN Controller Command Reference, Release 4.0*

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 3560 Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- *Catalyst 3560 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3560 Switch Getting Started Guide* (order number DOC-7816660=)
- *Regulatory Compliance and Safety Information for the Catalyst 3560 Switch* (order number DOC-7816665)

These documents provide complete information about the Catalyst 2970 switches:

- *Catalyst 2970 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 2970 Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- *Catalyst 2970 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2970 Switch Getting Started Guide* (order number DOC-7816685=)
- *Regulatory Compliance and Safety Information for the Catalyst 2970 Switch* (order number DOC-7816686=)

These documents provide complete information about the Catalyst 2960 switches:

- *Catalyst 2960 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide* (order number DOC-7816879=)



Note The above getting started guide, orderable in print, provides information in all supported languages. Listed below are online-only getting started guides in the individual languages.

- *Catalyst 2960 Switch Getting Started Guide*—English (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Chinese (Simplified) (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—French (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—German (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Italian (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Japanese (not orderable but available on Cisco.com)

- *Catalyst 2960 Switch Getting Started Guide*—Spanish (not orderable but available on Cisco.com)
- *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch* (order number DOC-7816880=)

For other information about related products, see these documents:

- Device manager online help (available on the switch)
- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide* (order number DOC-7810372=)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)
- These 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

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

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

© 2007 Cisco Systems, Inc. All rights reserved.