Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(35)SE and Later

Revised June 10, 2008

Cisco IOS Release 12.2(35)SE and SE1 run on all Catalyst 3750, 3560, 2970, and 2960 switches and on Cisco EtherSwitch service modules. Cisco IOS Release 12.2(35)SE5 runs on Catalyst 3750 switches and 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(35)SE and later and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 7.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 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 60.

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.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122srn.htm#wp2367913

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

Contents

This information is in the release notes:

System Requirements

The system requirements are described in these sections:

- "Hardware Supported" 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 on page 2 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

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 3750-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
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(35)SE
Catalyst 3560-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-48TS	48 10/100 ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24PS	24 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 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

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 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
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
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	Cisco IOS Release 12.2(18)SE
	100BASE-FX MMF[6]	Cisco IOS Release 12.2(20)SE
	GLC-BX-D , GLC-BS-U	Cisco IOS Release 12.2(35)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, XENPAK-10-GB-LX4, XENPAK-10-GB-SR, and XENPAK-10-GB-CX4	Cisco IOS Release 12.2(18)SE
Redundant power systems	Cisco RPS 675 Redundant Power SystemCisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch)	Supported on all software releases

[1] PoE = Power over Ethernet

[2] SFP = small form-factor pluggable

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

[4] Cisco EtherSwitch service module

[5] CWDM = coarse wavelength-division multiplexer

[6] MMF = multimode fiber

[7] XENPAK modules are only supported on the Catalyst 3750G-16TD switches.

Device Manager System Requirements

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

- "Hardware Requirements" 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

[1] We recommend Intel Pentium 4.

[2] 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(35)SE and later is only compatible with Cisco Network Assistant (CNA) 5.0 and later. You can download Cisco Network Assistant from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

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

Upgrading the Switch Software

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
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-i6l2-mz	c2970-lanbase-mz
c2970-i6k91l2-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.122-35.SE5.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.122-35.SE5.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.122-35.SE5.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.122-35.SE5.tar	Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules.
c3750-advipservicesk9-tar.122-35.SE5.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.

Table 5 Cisco IOS Software Image Files (continued)

Filename	Description
c3560-ipbase-tar.122-35.SE5.tar	Catalyst 3560 IP base image file and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3560-ipservices-tar.122-35.SE5.tar	Catalyst 3560 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3560-ipbasek9-tar.122-35.SE5.tar	Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3560-ipservicesk9-tar.122-35.SE5.tar	Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3560-advipservicesk9-tar.122-35.SE5.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.122-35.SE5.tar	Catalyst 2970 image file and device manager files. This image has Layer 2+ features.
c2970-lanbasek9-tar.122-35.SE5.tar	Catalyst 2970 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanbase-tar.122-35.SE5.tar	Catalyst 2960 image file and device manager files. This image has Layer 2+ features.
c2960-lanbasek9-tar.122-35.SE5.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

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/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt2/frf011.htm#wp1018426

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.122-35.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 13
- "Modifed Software Feature" section on page 13

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:

- Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled switch port. (Catalyst 3750 and 3560 switches)
- Support for IPv6 with Express Setup (Catalyst 3750 and 3560 switches)
- MAC inactivity aging to detect inactive hosts authenticated with MAC authentication bypass (MAB) and to remove them from an IEEE 802.1x-enabled port. (Catalyst 3750 and 3560 switches)
- Web authentication for authenticating a supplicant (client) that does not support IEEE 802.1x functionality (Catalyst 3750, 3560, and 2960 switches)
- Generic online diagnostics to test the hardware functionality of the supervisor engine (Catalyst 3560 switches only)
- HSRP enhanced object tracking (Catalyst 3750 and 3560 switches)
- Archive download enhancements for Catalyst 3750 switch stacks
- Configurable stack MAC persistent timer (Catalyst 3750 switches only)
- OSPF and EIGRP nonstop forwarding (NSF) capability that allows the switch to rebuild routing tables based on information from NSF-aware and NSF-capable neighbors (Catalyst 3750 switches IP services image only)

  Note NSF is not supported on interfaces running Hot Standby Routing Protocol (HSRP).

- IPv6 router ACL support in the IP services or IP base image for inbound management traffic on Layer 3 interfaces (Catalyst 3750 and 3560 switches)
- CISCO-POWER-ETHERNET-EXT-MIB support (Catalyst 3750 and 3560 switches)

Starting with Cisco IOS Release 12.2(25)SEE1, the device manager GUI, online help, and the *Catalyst 2960 Switch Getting Started Guide* are now available in Chinese (simplified), English, French, German, Italian, Japanese, and Spanish.

To display a translated version of the GUI and online help, select your language from the Language field located at the top of the device manager window.

The translated getting started guides are available at this URL:

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

Modifed Software Feature

The Catalyst 2960 device manager Dashboard window now displayed the Product ID and Version ID of the switch. The Product ID field replaced the Type field.

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
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
Support for IPv6 with Express Setup	12.2(35)SE	3750, 3560
Generic online diagnostics to test the hardware functionality of the supervisor engine.	12.2(35)SE	3560
Stack MAC persistent timer and archive download enhancements	12.2(35)SE	3750
HSRP enhanced object tracking	12.2(35)SE	3750, 3560
OSPF and EIGRP Nonstop forwarding capability (IP services image only)	12.2(35)SE	3750
IPv6 router ACLs for inbound Layer 3 management traffic in the IP base and IP services image	12.2(35)SE	3750, 3560
Generic online diagnostics to test the hardware functionality of the supervisor engine.	12.2(25)SEE	3750
DHCP Option 82 configurable remote ID and circuit ID	12.2(25)SEE	3750, 3560, 2970
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

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 802.1x inaccessible authentication bypass.	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x with restricted VLAN	12.2(25)SED	3750, 3560, and 2970 Cisco EtherSwitch service modules
Budgeting power for devices connected to PoE ports	12.2(25)SEC	3750 and 3560 Cisco EtherSwitch service modules
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEC 12.2(25)SED	3750, 3560, and 2970 Cisco EtherSwitch service modules 2960
Unique device identifier (UDI)	12.2(25)SEC	3750, 3560, 2970 Cisco EtherSwitch service modules
VRF Lite	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x with wake-on-LAN	12.2(25)SEC 12.2(25)SED	3750, 3560, 2970 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 12.2(25)SED	3750, 3560, 2970 Cisco EtherSwitch service modules
Secure Copy Protocol	12.2(25)SEC 12.2(25)SED	3750, 3560, 2970 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
IGMP snooping querier	12.2(25)SEA 12.2(25)FX	3750, 3560, 2970, and 2960
Advanced IP services	12.2(25)SEA	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
Support for DSCP transparency	12.2(25)SE 12.2(25)FX	3750, 3560, 2970, and 2960
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 12.2(25)FX	3750, 3560, 2970, and 2960
IEEE 802.1Q tunneling and Layer 2 protocol tunneling	12.2(25)SE	3750, 3560
Layer 2 point-to-point tunneling and Layer 2 point-to-point tunneling bypass	12.2(25)SE	3750, 3560
Support for SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE 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

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
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 30

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 18
- "Ethernet" section on page 20
- "Fallback Bridging" section on page 21
- "HSRP" section on page 21
- "IP" section on page 21
- "IP Telephony" section on page 21
- "MAC Addressing" section on page 22
- "Management" section on page 22
- "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 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 Mbps full duplex or 100 Mbps 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 Mbps 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 bps, 19200 bps, and 38400 bps) 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 Mbps instead of for 10/100 Mbps.
  - 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 IG MP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

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

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

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

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

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

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

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

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 boot 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 Mbps 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's active switch.

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:

  1. Choose **Tools** > **Internet Options**.
  2. Click **Settings** in the “Temporary Internet files” area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.

- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

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

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

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

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **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	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	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 Mbps 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.

- CSCsc30733

  This error message 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
  ```

  There is no workaround. However, this is only an informational message and does not affect switch functionality.

- 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.

- CSCse97398 (Catalyst 3750 and 3560 switches)

  Entering the **reload** privileged EXEC command might not reload the switch after these events occur in the order listed:

  a. An SNMP configuration file that contains `crypto key generate rsa` is copied to the switch running configuration.

  b. An **snmp set** command is performed.

  c. The **reload** command is entered.

  The workaround is to not copy an SNMP configuration with a configuration file that contains `crypto key generate rsa`. If the switch has existing keys, the Cisco IOS operating system expects either a *Yes* or *No* response that you want to replace the existing keys. If the switch does not have existing keys, the system expects the key size. The system never receives the *Yes* or *No* response nor the key size because the copy operation is performed from SNMP.

- Otherwise you can power-cycle the switch to clear the problem or enter the **clear configuration lock** privileged EXEC command to clear the system lockup and allow the **reload** command to execute.

- 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.

- CSCse01557 (Catalyst 3750 switches)

  The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear in 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.

- 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.

- 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.

- CSCsg18176 (Catalyst 3750 and 3560 switches)

  When dynamic ARP inspection is enabled and IP validation is disabled, the switch drops ARP requests that have a source address of 0.0.0.0.

  The workaround is to configure an ARP access control list (ACL) that permits IP packets with a source IP address of 0.0.0.0 (and any MAC) address) and apply the ARP ACL to the desired DAI VLANs.

- 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.

- CSCsg30295

  When you configure an IP address on a switch virtual interface (SVI) with DCHP and enable DHCP snooping on the SVI VLAN, the switch SVI cannot obtain an IP address.

  The workaround is to not enable DCHP snooping on the SVI VLAN or to use a static IP address for the SVI.

- 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.

  CSCsg70039 (Catalyst 3750 and 3560 switches)

  When both an authorized data domain and an authorized voice domain is present on a port, and you change the VLAN configuration on the port to equal the assigned VLAN, a traceback error appears. This problem only occurs on the ports of a member switch.

  The workaround is to change the voice VLAN to a value that does not match the assigned VLAN or VLAN feature (such as a guest VLAN).

- 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.

- CSCsg94672 (Catalyst 3750 and 3560 switches)

  An IEEE 802.1x port configured for Multi-Domain Authentication does not allow access to the guest VLAN if an IEEE 802.1x supplicant has previously authenticated and then logged off.

  On a Catalyst 3750 or Catalyst 3560 switch running Cisco IOS Release 12.2(35)SE or later, when an 802.1x port is configured for Multi-Domain Authentication and Guest VLAN, the guest VLAN feature is disabled once an 802.1X-enabled client has attached on the port. The feature remains disabled until the link goes down on the port. The result is that if an IEEE802.1x-enabled host is attached to the switch through an IP phone and is later replaced by a non-IEEE802.1x enabled host, the new host is not able to access the network via the guest VLAN. Instead, the port keeps trying to authenticate the new host (via IEEE802.1x or MAC Authentication Bypass indefinitely.

  The workaround is to enter the **dot1x guest-vlan supplicant** global configuration command to allow access to the guest VLAN even after EAPoL packets have been seen on a port.

Resolved Caveats

This sections describes the caveats that have been resolved in this release:

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

- "Caveats Resolved in Cisco IOS Release 12.2(35)SE5" section on page 37
- "Resolved Caveats in Cisco IOS Release 12.2(35)SE2" section on page 38
- "Resolved Caveats in Cisco IOS Release 12.2(35)SE1" section on page 39
- "Resolved Caveats in Cisco IOS Release 12.2(35)SE" section on page 39

Caveats Resolved in Cisco IOS Release 12.2(35)SE5

- CSCed87897

  The output of the **show ip route** privileged EXEC command now correctly displays the default gateway.

- CSCsh90678 (Catalyst 3750 switches)

  The stack master switch no longer resets with an error message when you enter the **show storm-control** user EXEC command and specify a stack member interface that is not configured for storm control.

- CSCsh89429

  The switch no longer reloads when the **write core** privileged EXEC command is entered when testing a core dump configuration and FTP is selected as the file transfer protocol.

- CSCsi74508

  A switch no longer displays this error message when reading from or writing to the configuration file:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: write of 11 bytes to 10 bytes
  -Traceback= 0x41186A90 0x411A3960 0x411C1F88 0x413C24B8 0x4031EEDC 0x4032D144
  0x411C3974 0x41193D9C 0x4119420C 0x411DF55C 0x411C70AC 0x411E3184 0x425590F4
  0x4254BD7C 0x421B5CE0 0x421B5CC4
  ```

- CSCsi94450

  When DHCP snooping is enabled on a VLAN, the broadcast DHCP request is now correctly sent over the trusted port and the connected hosts correctly receive their IP addresses.

Resolved Caveats in Cisco IOS Release 12.2(35)SE2

These caveats were resolved in Cisco IOS Release 12.2(35)SE2:

- 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.

- CSCsg89979 (Catalyst 3750 switches)

  A Gigabit Ethernet port on a Catalyst 3750 switch running Cisco IOS Release 12.2(35)SE1 shows linkup but no data goes through the port, including pinging the host through the port. This problem is fixed in Cisco IOS Release 12.2(35)SE2.

- CSCsh11040 (Catalyst 3750 switches)

  On a Catalyst 3750 switch, changing the MAC address or VLAN ID associated with an IPv4 or IPv6 address present in the ARP table or neighbor table no longer might impact traffic forwarding.

Resolved Caveats in Cisco IOS Release 12.2(35)SE1

These caveats were resolved in Cisco IOS Release 12.2(35)SE1:

- CSCse03859 (Catalyst 2960 switches)

  DHCP snooping now works when the switch is in VTP server mode and VLANs with IDs greater than 255 (256 and above) are created.

- CSCsg98846 (Catalyst 3750 and 3560 switches)

  When multiple hosts are authenticated on an IEEE 802.1X-enabled port that is configured with multidomain authentication (MDA), a START/STOP RADIUS Attribute-Value (AV) pair is now sent for each host.

- CSCsh04783 (Catalyst 3750 and 3560 switches)

  Access control lists that are applied to routed ports on a member switch are now programmed into the switch hardware.

- CSCsg98527 (Catalyst 3750 and 3560 switches)

  The MAC access bypass (MAB) inactivity timer is no longer applied to an IP phone (Cisco or non-Cisco) connected to an IEEE 802.1x-enabled port that is configured with multidomain authentication (MDA).

- CSCsh15007 (Catalyst 2960G switches)

  A query of the SNMP MIB object chassisFanStatus.0 no longer returns a value of *4* (which indicates that the fan is faulty) when the fan is operating properly.

Resolved Caveats in Cisco IOS Release 12.2(35)SE

These caveats were resolved in Cisco IOS Release 12.2(35)SE:

- CSCeh95744

  If two or more switches in a stack of PoE switches restarted at the same time and you entered the **no switch stack-member-number provision** global configuration command, this message no longer appears on the console:

  ```
  %Command not applied to switch x, remote error
  ```

- CSCei63394

  When an IEEE 802.1x restricted VLAN is configured on a port and a hub with multiple devices are connected to that port, syslog messages are now generated.

  This is not a supported configuration. Only one host should be connected to an IEEE 802.1x restricted VLAN port.

- CSCei79428 (Catalyst 3750 switches)

  When a switch joins a stack running Cisco IOS 12.2(20)SE1 or earlier, the **boot auto-copy-sw** now works correctly.

- CSCeh35693 (Cisco EtherSwitch service modules)

  If two Cisco EtherSwitch service modules were directly connected through Fast Ethernet interfaces configured as both 100 Mbps and full duplex *and* as automatic speed and duplex settings, one interface might have detected the other as a Cisco-powered device.

- 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.

- CSCsb56438

  An extra index no longer appears in the port table of the ciscoStpExtensions MIB.

- CSCsb58462

  When a stack of Catalyst 3750 switches are configured with a Layer 3 LACP EtherChannel, tracebacks are no longer generated when a stack master failover occurred.

- CSCsb60164

  When a Catalyst 3750 stack master fails or leaves the stack, a cross-stack EtherChannel in trunk mode running Link Aggregation Control Protocol (LACP) protocol no longer stops forwarding traffic on some VLANs.

- CSCsb74648

  When a Cisco device is configured for Network Admission Control and the EAP over UDP port number changes from its default value and then changes back with the *eou* default switch configuration command, the port change now takes effect.

- CSCsb75245

  When you configure a Cisco IP Phone to use Network Admission Control, the CDP packet is no longer delayed, and the phone is no longer identified as an agentless host without an identity profile.

- CSCsb81023 (Catalyst 3750 switches)

  A nonstackable EtherSwitch Service Module no longer boots with this provisioned switch error message:

```
switch 1 provision NME-X-23ES-1G-P
                ^
% Invalid input detected at '^' marker.
Failed to generate persistent self-signed certificate.
Secure server will use temporary self-signed certificate.
```

- CSCsc05371

  When you configure a MAC address filter by entering the **mac-address-table static vlan drop** global configuration command, IEEE 802.1X no longer authenticates supplicants using that address. If a supplicant with that address is authenticated, its authorization is revoked.

- CSCsc29225

  When you remove the bridge topology change trap with the **no snmp-server enable traps bridge topologychange** configuration command, the stpx root-inconsistency trap is now active.

- CSCsc55332 (Cisco EtherSwitch service modules)

  When reloading a Cisco EtherSwitch service module that is a member of a switch stack and port security is enabled on the stack, a `PSECURE` traceback error no longer appears.

- CSCsc88760 (Catalyst 3750 switches)

  When you reload the stack master and a stack member at the same time, the entPhysicalIndex in the entPhysicalTable (ENTITY-MIB) for the SFP modules is now correct.

- CSCsc93768 (Catalyst 3750 and 3560 switches)

  A switch no longer fails when the VPN Routing and Forwarding (VRF) configuration is removed under these conditions (in this order):

  - Interfaces are configured in two or more VRFs.
  - One VRF has static address resolution protocols (ARPs) configured.
  - The VRF configuration with static ARPs is removed.
  - The second VRF configuration is removed.

  VRF is removed by using the **no ip vrf** global configuration command.

- CSCsd12172 (Catalyst 3750, 3560, and 2970 switches)

  When the switch is running Ethernet over multiprotocol label switching (EoMPLS) in Cisco IOS Release 12.2(25)SED, the switch virtual interface (SVI) service policy now polices data traffic according to its defined policy.

- CSCsd17229 (Catalyst 3750 switches)

  When you reload a switch stack, the SFP module information now appears in the entPhysicalTable (ENTITY-MIB).

- CSCsd46042

  If you insert a defective SFP module into the switch SFP module slot, HSRP links flap and CPUHOG error messages are no longer sent.

- CSCsd62507 (Catalyst 3750 and 3560 switches)

  When you clear the ARP by entering the **clear arp user [interface <name>]** EXEC command or when the ARP entry times out, the switch now sends packets with the correct destination MAC address.

- CSCsd78044 (Catalyst 3750 and 3560 switches)

  When IGMP snooping is enabled and an EtherChannel member interface goes down, the switch now forwards multicast traffic on the rest of the EtherChannel member interfaces.

- CSCsd79916

  When IEEE 802.1x authentication was configured on a voice VLAN port, the switch did not forward traffic if the attached PC was configured for both machine authentication and user authentication.

  An authenticated 802.1X port might not have forwarded traffic in these conditions:

  - The port is assigned to a voice VLAN.
  - The PC is configured for both machine authentication and user authentication.
  - The machine-initiated and user-initiated authentications result in different VLANs being assigned to the port.

- CSCsd84624 (Catalyst 3750 and 3560 switches)

  Sometimes the switch dropped a fragmented multicast packet when it did not have the (S,G) entry, and more than 600 packets per second (pps) of other multicast traffic were sent to the switch CPU.

- CSCsd85770 (Catalyst 2960G switches)

  When you apply the **mls qos trust dscp** global configuration command to a port, this error message no longer appears:

  ```
  Master sets trust failed, sets to untrust modetrust type update
  failed on ifc GigabitEthernetx/x
  Switch(config-if)#Tcam write failed trust dscp
  %QOSMGR-4-COMMAND_FAILURE: Execution of slave:HQM_IDBTRUST_CMD
  command failed on GigabitEthernetx/x
  ```

- CSCsd86177

  When you remove and reconfigure a loopback interface, it no longer appears in the ifTable.

- CSCsd87313 (Catalyst 3750 switches)

  When you configure the **ip cef load-sharing algorithm universal** <*id*> global configuration command on the master switch, the command now appears in the stack member's running configuration. If the command is not configured on the master, it does not appear on the stack member switches.

- CSCsd88924

  The output from the **show interface** global configuration command now shows private VLANs for notconnect ports.

- 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.

- CSCsd93596 (Catalyst 3750 switches)

  EtherChannels with very long allowed VLAN lists no longer experience a link flap when a master failover occurs.
- CSCse03570 (Catalyst 3750 switches)

  A routing protocol flap no longer occurs when a stack member joins the stack.
- CSCsd08314

  When you remove a voice VLAN that has no per-VLAN configuration from a secure port, a `PORT_SECURITY-6-VLAN_REMOVED` message no longer appears.

  Note: If an address was learned on a VLAN, the error message still appears when that VLAN is aged out or removed. However, this does not affect switch functionality.
- CSCse14774

  If a switch is connected to a third-party router through an EtherChannel and the EtherChannel is running in Link Aggregation Control Protocol (LACP) mode, the interfaces in the EtherChannel no longer fail after you enter the **switchport trunk native vlan** *vlan-id* interface configuration command to change the native VLAN from VLAN 1 (the default) to a different VLAN ID.
- CSCse21219

  If a Putty client is used to change the configuration to a device with SSH, the switch no longer stops responding to incoming traffic, such as SSH, Telnet, or ping packets.
- CSCse22188 (Catalyst 3750 and 3560 switches)

  If fallback bridging is enabled on a routed port connected to an IEEE 802.1Q trunk port that is an EtherChannel member, the EtherChannel is no longer disabled after receiving the DTP frames.
- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

Documentation Updates

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

- EtherChannel Update, page 45
- Updates for the System Message Guide, page 45
- Update to the Catalyst 2960 Software Configuration Guide, page 45

- Update to the Catalyst 2960 Command Reference, page 48
- show fallback profile, page 53
- Updates for the Regulatory Compliance and Safety Information, page 57

EtherChannel Update

When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. In previous releases, the incompatible ports were suspended. Beginning with Cisco IOS Release 12.2(35)SE, instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

Updates for the System Message Guide

For new messages in this release, see the Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide, 12.2(35)SE at this URL:
http://www.cisco.com/en/US/products/hw/switches/ps5023/products_system_message_guides_list.html

Update to the Catalyst 2960 Software Configuration Guide

These sections were added to the "Configuring IEEE 802.1x" chapter:

Using Web Authentication

You can use a web browser to authenticate a client that does not support IEEE 802.1x functionality.

You can configure a port to use only web authentication. You can also configure the port to first try and use IEEE 802.1x authentication and then to use web authorization if the client does not support IEEE 802.1x authentication.

Web authentication requires two Cisco Attribute-Value (AV) pair attributes:

- The first attribute, priv-lvl=15, must always be set to *15*. This sets the privilege level of the user who is logging into the switch.
- The second attribute is an access list to be applied for web authenticated hosts. The syntax is similar to IEEE 802.1X per-user ACLs. However, instead of ip:inacl, this attribute must begin with proxyacl, and the source field in each entry must be any. (After authentication, the client IP address replaces the any field when the ACL is applied.)

  For example:

```
proxyacl# 10=permit ip any 10.0.0.0 255.0.0.0
proxyacl# 20=permit ip any 11.1.0.0 255.255.0.0
proxyacl# 30=permit udp any any eq syslog
proxyacl# 40=permit udp any any eq tftp
```

Note The *proxyacl* entry determines the type of allowed network access.

For more information, see the "Configuring Web Authentication" section on page 46.

Configuring Web Authentication

Beginning in privileged EXEC mode, follow these steps to configure authentication, authorization, accounting (AAA) and RADIUS on a switch before configuring web authentication. The steps enable AAA by using RADIUS authentication and enable device tracking.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

Step 3	**aaa authentication login default group radius**	Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see the *Catalyst 2960 Software Configuration Guide*.
		The console prompts you for a username and password on future attempts to access the switch console after entering the **aaa authentication login** command. If you do not want to be prompted for a username and password, configure a second login authentication list:
		`Switch#` **`config t`**
		`Switch(config)#` **`aaa authentication login line-console none`**
		`Switch(config)#` **`line console 0`**
		`Switch(config-line)#` **`login authentication line-console`**
		`Switch(config-line)#` **`end`**

Step 4	**aaa authorization auth-proxy default group radius**	Use RADIUS for authentication-proxy (auth-proxy) authorization.
Step 5	**radius-server host key** *radius-key*	Specify the authentication and encryption key for RADIUS communication between the switch and the RADIUS daemon.
Step 6	**radius-server attribute 8 include-in-access-req**	Configure the switch to send the Framed-IP-Address RADIUS attribute (Attribute[8]) in access-request or accounting-request packets.
Step 7	**radius-server vsa send authentication**	Configure the network access server to recognize and use vendor-specific attributes (VSAs).
Step 8	**ip device tracking**	Enable the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration commands.
Step 9	**end**	Return to privileged EXEC mode.

This example shows how to enable AAA, use RADIUS authentication and enable device tracking:

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
Switch(config)# radius-server host key key1
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# radius-server vsa send authentication
Switch(config)# ip device tracking
Switch(config) end
```

Beginning in privileged EXEC mode, follow these steps to configure a port to use web authentication:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip admission name** *rule* **proxy http**	Define a web authentication rule. **Note** The same rule cannot be used for both web authentication and NAC Layer 2 IP validation.
Step 3	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 4	**switchport mode access**	Set the port to access mode.
Step 5	**ip access-group** *access-list* **in**	Specify the default access control list to be applied to network traffic before web authentication.
Step 6	**ip admission** *rule*	Apply an IP admission rule to the interface.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config interface** *interface-id*	Verify your configuration.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure only web authentication on a switch port:

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# ip access-group policy1 in
Switch(config-if)# ip admission rule1
Switch(config-if)# end
```

Beginning in privileged EXEC mode, follow these steps to configure a switch port for IEEE 802.1x authentication with web authentication as a fallback method:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip admission name** *rule* **proxy http**	Define a web authentication rule.
Step 3	**fallback profile** *fallback-profile*	Define a fallback profile to allow an IEEE 802.1x port to authenticate a client by using web authentication.
Step 4	**ip access-group** *policy* **in**	Specify the default access control list to apply to network traffic before web authentication.
Step 5	**ip admission** *rule*	Associate an IP admission rule with the profile, and specify that a client connecting by web authentication uses this rule.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 8	**switchport mode access**	Set the port to access mode.
Step 9	**dot1x port-control auto**	Enable IEEE 802.1x authentication on the interface.

	Command	Purpose
Step 10	**dot1x fallback** *fallback-profile*	Configure the port to authenticate a client by using web authentication when no IEEE 802.1x supplicant is detected on the port. **Note** Web authorization cannot be used as a fallback method for IEEE 802.1x if the port is configured for multidomain authentication.
Step 11	**exit**	Return to privileged EXEC mode.
Step 12	**show dot1x interface** *interface-id*	Verify your configuration.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback method.

```
Switch(config) configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile fallback1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabit1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback fallback1
Switch(config-if)# end
```

For more information about the **ip admission name** and **dot1x fallback** commands, see the command reference for this release.

Update to the Catalyst 2960 Command Reference

These commands were added:

- "dot1x fallback" section on page 48
- "fallback profile" section on page 49
- "ip admission" section on page 51
- "ip admission name proxy http" section on page 52
- "show fallback profile" section on page 53

dot1x fallback

Use the **dot1xfallback** interface configuration command on the switch stack or on a standalone switch to configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication. To return to the default setting, use the **no** form of this command.

dot1x fallback *fallback-profile*

no dot1x fallback

Syntax Description

fallback-profile	Specify a fallback profile for clients that do not support IEEE 802.1x authentication.

Defaults

No fallback is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

You must enter the **dot1x port-control** auto interface configuration command on a switch port before entering this command.

Examples

This example shows how to specify a fallback profile to a switch port that has been configured for IEEE 802.1x authentication:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# dot1x fallback profile1
Switch(config-fallback-profile)# exit
Switch(config)# end
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
show dot1x[**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a port
ip admission name proxy http	Enable web authentication globally on a switch

fallback profile

Use the **fallback profile** global configuration command on the switch stack or on a standalone switch to create a fallback profile for web authentication. To return to the default setting, use the **no** form of this command.

fallback profile *profile*

no fallback profile

Syntax Description

profile	Specify the fallback profile for clients that do not support IEEE 802.1x authentication.

Defaults

No fallback profile is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The fallback profile is used to define the IEEE 802.1x fallback behavior for IEEE 802.1x ports that do not have supplicants. The only supported behavior is to fall back to web authentication.

After entering the **fallback profile** command, you enter profile configuration mode, and these configuration commands are available:

- **ip:** Create an IP configuration.
- **access-group:** Specify access control for packets sent by hosts that have not yet been authenticated.
- **admission:** Apply an IP admission rule.

Examples

This example shows how to create a fallback profile to be used with web authentication:

```
Switch# configure terminal
Switch(config)# ip admission name rule1 proxy http
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip access-group default-policy in
Switch(config-fallback-profile)# ip admission rule1
Switch(config-fallback-profile)# exit
Switch(config)# interface gigabitethernet 1/0/1
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

You can verify your settings by entering the **show running-configuration** [**interface** *interface-id*] privileged EXEC command.

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.
show fallback profiles	Display the configured profiles on a switch.

ip admission

Use the **ip admission** interface configuration command to enable web authentication. You can also use this command in fallback-profile mode. Use the **no** form of this command to disable web authentication.

ip admission *rule*

no ip admission

Syntax Description

rule	Apply an IP admission rule to the interface.

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

Examples

This example shows how to apply a web authentication rule to a switchport:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config)# ip admission name rule1
Switch(config)# end
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Enable web authentication on a port
ip admission name proxy http	Enable web authentication globally on a switch
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the *Network Admission Control Software Configuration Guide* on Cisco.com.

ip admission name proxy http

Use the **ip admission name proxy http** global configuration command to enable web authentication. Use the **no** form of this command to disable web authentication.

ip admission name *proxy http*

no ip admission name *proxy htt***p**

Syntax Description

This command has no arguments or keywords.

Defaults

Web authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

The **ip admission name proxy http** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission** *web-rule* interface configuration commands to enable web authentication on a specific interface.

Examples

This example shows how to configure only web authentication on a switchport:

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switchport.

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a port
show ip admission	Displays information about NAC cached entries or the NAC configuration. For more information, see the *Network Admission Control Software Configuration Guide* on Cisco.com.

show fallback profile

Use the **show fallback profile** privileged EXEC command to display the fallback profiles that are configured on a switch.

show fallback profile [append | begin | exclude | include | {[redirect | tee] *url*} *expression*]

Syntax Description

| append	(Optional) Append redirected output to a specified URL
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
| redirect	(Optional) Copy output to a specified URL.
| tee	(Optional) Copy output to a specified URL.
expression	Expression in the output to use as a reference point.
url	Specified URL where output is directed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(35)SE	This command was introduced.

Usage Guidelines

Use the **show fallback** profile privileged EXEC command to display profiles that are configured on the switch.

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

Examples

This is an example of output from the **show fallback profile** command:

```
switch# show fall profile
Profile Name: dot1x-www
------------------------------------
Description       : NONE
IP Admission Rule : webauth-fallback
IP Access-Group IN: default-policy
Profile Name: dot1x-www-lpip
------------------------------------
Description       : NONE
IP Admission Rule : web-lpip
IP Access-Group IN: default-policy
Profile Name: profile1
------------------------------------
Description       : NONE
IP Admission Rule : NONE
IP Access-Group IN: NONE
```

Related Commands

Command	Description
dot1x fallback	Configure a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
fallback profile	Create a web authentication fallback profile.
ip admission	Enable web authentication on a switch port
ip admission name proxy http	Enable web authentication globally on a switch
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

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 Make sure that nothing is connected to the switch.

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.

Step 2 Power the switch by connecting the supplied AC power cord to the switch power connector and to a grounded AC outlet.

Step 3 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.

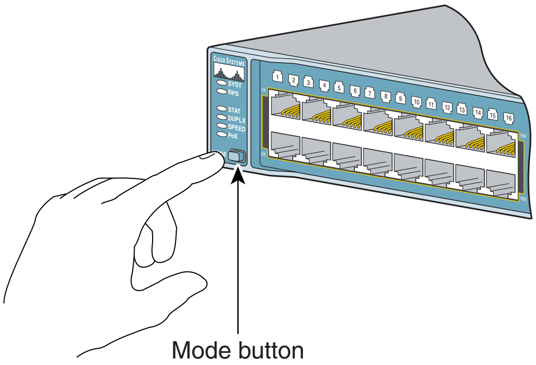
Wait for the switch to complete POST, which can take several minutes.

Step 4 Verify that POST has completed by confirming that the SYST LED remains green. If the switch fails POST, the SYST LED turns amber.

POST errors are usually fatal. Contact your Cisco technical support representative if your switch fails POST.

Step 5 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.

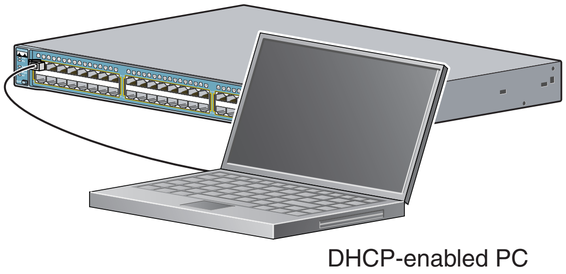
If the LEDs left of the Mode button begin to blink after you press the button, release it. Blinking LEDs mean that the switch has already been configured and cannot go into Express Setup mode. For more information, see the "Resetting the Switch" section.



Step 6 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.)

Step 7 Connect a Category 5 Ethernet cable to any 10/100 or 10/100/1000 Ethernet port on the switch front panel.

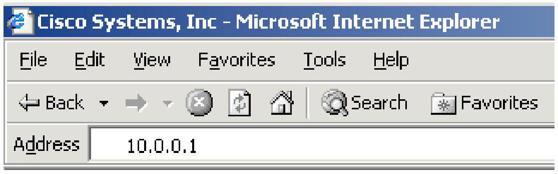
Connect the other end of the cable to the Ethernet port on your PC.



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

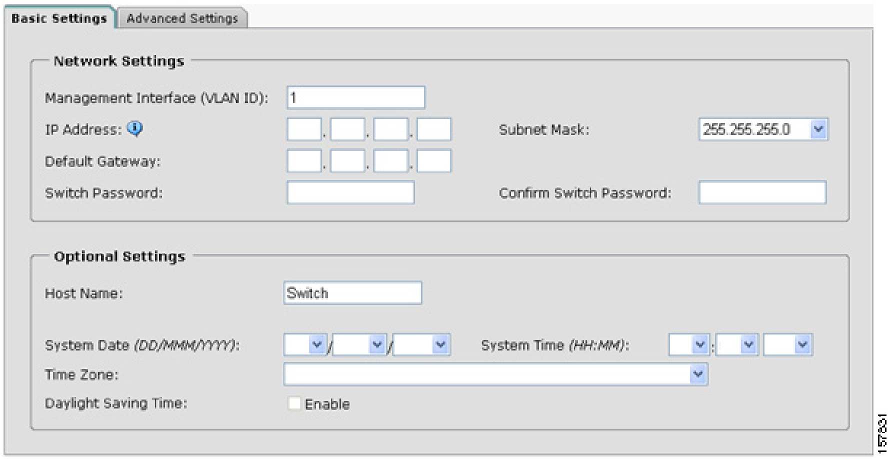
Wait 30 seconds.

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


Cisco Systems, Inc - Microsoft Internet Explorer

Address 10.0.0.1

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



Network Settings

Management Interface (VLAN ID): 1

IP Address: . . .

Subnet Mask: 255.255.255.0

Default Gateway: . . .

Switch Password:

Confirm Switch Password:

Optional Settings

Host Name: Switch

System Date *(DD/MMM/YYYY)*: / /

System Time *(HH:MM)*: :

Time Zone:

Daylight Saving Time: □ Enable

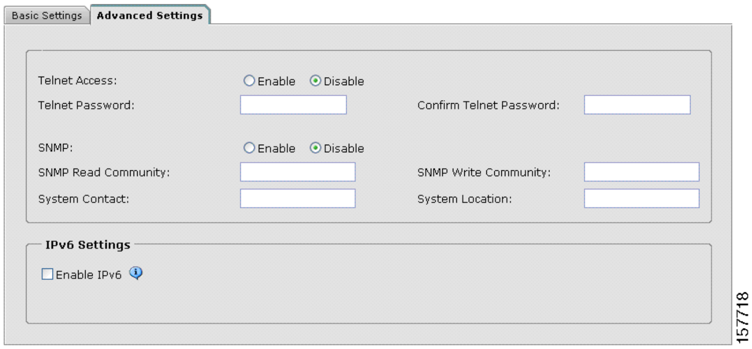
Step 10 Enter this information in the **Network Settings** fields:

- 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.



Telnet Access: ○ Enable ● Disable
Telnet Password:
Confirm Telnet Password:
SNMP: ○ Enable ● Disable
SNMP Read Community:
SNMP Write Community:
System Contact:
System Location:

IPv6 Settings
□ Enable IPv6

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 for the Regulatory Compliance and Safety Information

This information was added to the *Regulatory Compliance and Safety Information* for the Catalyst 3750, 3560, 2970, and 2960 switches.

Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails

Warning **Voice over IP (VoIP) service and the emergency calling service do not function if power fails or is disrupted. After power is restored, you might have to reset or reconfigure equipment to regain access to VoIP and the emergency calling service. In the USA, this emergency number is 911. You need to be aware of the emergency number in your country.** Statement 361

Waarschuwing **Voice over IP (VoIP)-service en de service voor noodoproepen werken niet indien er een stroomstoring is. Nadat de stroomtoevoer is hersteld, dient u wellicht de configuratie van uw apparatuur opnieuw in te stellen om opnieuw toegang te krijgen tot VoIP en de noodoproepen. In de VS is het nummer voor noodoproepen 911. U dient u zelf op de hoogte te stellen van het nummer voor noodoproepen in uw land.**

Varoitus **Voice over IP (VoIP) -palvelu ja hätäpuhelupalvelu eivät toimi, jos virta katkeaa tai sen syötössä esiintyy häiriöitä. Kun virransyöttö on taas normaali, sinun täytyy mahdollisesti asettaa tai määrittää laitteisto uudelleen, jotta voisit jälleen käyttää VoIP-palvelua ja hätäpuhelupalvelua. Yhdysvalloissa hätänumero on 911. Selvitä, mikä on omassa kotimaassasi käytössä oleva hätänumero.**

Attention **Le service Voice over IP (VoIP) et le service d'appels d'urgence ne fonctionnent pas en cas de panne de courant. Une fois que le courant est rétabli, vous devrez peut-être réinitialiser ou reconfigurer le système pour accéder de nouveau au service VoIP et à celui des appels d'urgence. Aux États-Unis, le numéro des services d'urgence est le 911. Vous devez connaître le numéro d'appel d'urgence en vigueur dans votre pays.**

Warnung **Bei einem Stromausfall oder eingeschränkter Stromversorgung funktionieren VoIP-Dienst und Notruf nicht. Sobald die Stromversorgung wieder hergestellt ist, müssen Sie möglicherweise die Geräte zurücksetzen oder neu konfigurieren, um den Zugang zu VoIP und Notruf wieder herzustellen. Die Notrufnummer in den USA lautet 911. Wählen Sie im Notfall die für Ihr Land vorgesehene Notrufnummer.**

Avvertenza **Il servizio Voice over IP (VoIP) e il servizio per le chiamate di emergenza non funzionano in caso di interruzione dell'alimentazione. Ristabilita l'alimentazione, potrebbe essere necessario reimpostare o riconfigurare l'attrezzatura per ottenere nuovamente l'accesso al servizio VoIP e al servizio per le chiamate di emergenza. Negli Stati Uniti, il numero di emergenza è 911. Si consiglia di individuare il numero di emergenza del proprio Paese.**

Advarsel **Tjenesten Voice over IP (VoIP) og nødanropstjenesten fungerer ikke ved strømbrudd. Etter at strømmen har kommet tilbake, må du kanskje nullstille eller konfigurere utstyret på nytt for å få tilgang til VoIP og nødanropstjenesten. I USA er dette nødnummeret 911. Du må vite hva nødnummeret er i ditt land.**

Aviso **O serviço Voice over IP (VoIP) e o serviço de chamadas de emergência não funcionam se houver um corte de energia. Depois do fornecimento de energia ser restabelecido, poderá ser necessário reiniciar ou reconfigurar o equipamento para voltar a utilizar os serviços VoIP ou chamadas de emergência. Nos EUA, o número de emergência é o 911. É importante que saiba qual o número de emergência no seu país.**

¡Advertencia! **El servicio de voz sobre IP (VoIP) y el de llamadas de emergencia no funcionan si se interrumpe el suministro de energía. Tras recuperar el suministro es posible que deba que restablecer o volver a configurar el equipo para tener acceso a los servicios de VoIP y de llamadas de emergencia. En Estados Unidos el número de emergencia es el 911. Asegúrese de obtener el número de emergencia en su país.**

Varning! **Tjänsten Voice over IP (VoIP) och larmnummertjänsten fungerar inte vid strömavbrott. Efter att strömmen kommit tillbaka måste du kanske återställa eller konfigurera om utrustningen för att få tillgång till VoIP och larmnummertjänsten. I USA är det här larmnumret 911. Du bör ta reda på det larmnummer som gäller i ditt land.**

Az IP csatornán történő hangátvitel (VoIP) és a segélyhívó szolgáltatás nem működik, ha az áramellátás megszűnik vagy megszakad. Az áramellátás helyreállítását követően előfordulhat, hogy alaphelyzetbe kell állítani vagy újra kell konfigurálni a berendezést, hogy újra hozzáférhessen a VoIP és a segélyhívó szolgáltatáshoz. Az Egyesült Államokban a segélyhívó szám 911. Tisztában kell lennie a saját országának segélyhívó számával.

Предупреждение **Служба передачи голоса по IP (VoIP) и служба экстренных вызовов не будут работать, если произошел сбой питания. После восстановления питания, возможно, потребуется перенастроить оборудование, чтобы возобновить доступ к службе VoIP и службе экстренных вызовов. В США телефон службы экстренных вызовов 911. Вам необходимо знать телефон этой службы в своей стране.**

警告 如果电源出现故障或中断，您将无法使用 Voice over IP (VoIP) 服务与紧急呼叫服务。电源恢复之后，您可能需要重新设置或重新配置设备，以便重新获得进入 VoIP 与紧急呼叫服务的权限。在美国，此紧急呼叫号码是 911。您必须知道本国的紧急呼叫号码。

警告 電源障害や停電の場合、ボイス オーバー アイピー (VoIP) サービスと緊急呼出しサービスは機能しません。電源の回復後、VoIP と緊急呼出しサービスにアクセスするには機器をリセットまたは再設定する必要があります。米国内の緊急呼出し番号は 911 です。お住まいの地域の緊急呼出し番号をあらかじめ調べておいてください。

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 listed in the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page 62.

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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