Release Notes for the Catalyst 2955, Catalyst 2950, and Catalyst 2940 Switches, Cisco IOS Release 12.1(22)EA7

Eebruary 1, 2006

Cisco IOS Release 12.1(22)EA7 runs on Catalyst 2955, Catalyst 2950, and Catalyst 2940 switches.

Review the new software features, open caveats, and resolved caveats sections for information specific to your switch. The information in this document refers to all the switches, unless otherwise noted.

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. To verify that these are the correct release notes 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 running, you can use the **show version** user 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 Cisco IOS version.

For the complete list of Catalyst 2955, Catalyst 2950, and Catalyst 2940 switch documentation, see the "Related Documentation" section on page 54.

You can download the switch software from this site:

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

This Cisco IOS 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 Cisco IOS releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Cisco IOS Release 12.1(22)EA7 is based on Cisco IOS Release 12.1(22)E7. Open caveats in Cisco IOS Release 12.1(22)E7 also affect Cisco IOS Release 12.1(22)EA7 unless they are listed in the Cisco IOS Release 12.1(22)EA7 resolved caveats list. The list of open caveats in Cisco IOS Release 12.1(22)E7 is available at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/ol_2310.htm#wp1560107

Cisco Systems

Corporate 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 for this release are described in these sections:

Hardware Supported

The Catalyst 2950 switch is supported by either the standard software image (SI) or the enhanced software image (EI). The Catalyst 2950 Long-Reach Ethernet (LRE) and Catalyst 2955 switches are supported only by the EI. The Catalyst 2940 switch supports some of the features supported by a Catalyst 2950 switch.

The EI provides a richer set of features, including access control lists (ACLs), enhanced quality of service (QoS) features, and extended-range VLANs. The cryptographic SI and EI support the Secure Shell Version 2 (SSHv2) protocol.

For information about the software releases that support the switches listed in Table 1, see the "Catalyst 2950 Hardware and Software Compatibility Matrixes" section on page 24.

Table 1 and Table 2 list the hardware supported by this software release:

Table 1 Catalyst 2940, Catalyst 2950, and Catalyst 2955 Hardware Supported

Hardware	Software Image	Description
Catalyst 2940-8TT-S	–[1]	8 10/100 Ethernet ports and 1 10/100/1000 Ethernet port
Catalyst 2940-8TF-S	–[1]	8 10/100 Ethernet ports, 1 SFP[2] module slot, and 1 100BASE-FX port
Catalyst 2950-12	SI	12 fixed autosensing 10/100 Ethernet ports
Catalyst 2950-24	SI	24 fixed autosensing 10/100 Ethernet ports
Catalyst 2950C-24	EI	24 fixed autosensing 10/100 Ethernet ports and 2 100BASE-FX ports
Catalyst 2950G-12-EI	EI	12 fixed autosensing 10/100 Ethernet ports and 2 GBIC[3] module slots
Catalyst 2950G-24-EI	EI	24 fixed autosensing 10/100 Ethernet ports and 2 GBIC module slots
Catalyst 2950G-24-EI-DC	EI	24 fixed autosensing 10/100 Ethernet ports and 2 GBIC module slots with DC-input power
Catalyst 2950G-48-EI	EI	48 fixed autosensing 10/100 Ethernet ports and 2 GBIC module slots
Catalyst 2950ST-8 LRE	EI	8 LRE ports, 2 10/100/1000 Ethernet ports[4], and 2 SFP module slots
Catalyst 2950ST-24 LRE	EI	24 LRE ports, 2 10/100/1000 Ethernet ports[4], and 2 SFP module slots
Catalyst 2950ST-24 LRE 997	EI	24 LRE ports, 2 10/100/1000 Ethernet ports[4], and 2 SFP module slots with DC-input power
Catalyst 2950SX-24	SI	24 fixed autosensing 10/100 Ethernet ports and 2 1000BASE-SX ports
Catalyst 2950SX-48-SI	SI	48 fixed autosensing10/100 Ethernet ports and 2 1000BASE-SX ports
Catalyst 2950T-24	EI	24 fixed autosensing 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports[5]
Catalyst 2950T-48-SI	SI	48 fixed autosensing 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports
Catalyst 2955C-12	EI	12 fixed autosensing 10/100 ports and 2 MM[6] 100BASE-FX ports
Catalyst 2955S-12	EI	12 fixed autosensing 10/100 ports and 2 SM[7] 100BASE-LX ports
Catalyst 2955T-12	EI	12 fixed autosensing 10/100 ports and 2 10/100/1000 Ethernet ports[4]

1. The Catalyst 2940 switch supports some of the features supported by a Catalyst 2950 switch.
2. SFP = small form-factor pluggable
3. GBIC = Gigabit Interface Converter
4. The 10/100/1000 ports on a Catalyst 2950 LRE or Catalyst 2955T-12 switch operate at 10 or 100 Mbps in either full- or half-duplex mode and at 1000 Mbps only in full-duplex mode.
5. The 10/100/1000 interfaces on the Catalyst 2950T-24 switch do not support the **half** keyword in the **duplex** command.
6. MM = multimode
7. SM = single mode

Table 2 Other Hardware Supported

Hardware	Software Image	Description
Cisco 575 LRE CPE[1]	–	1 fixed 10/100 port
Cisco 576 LRE CPE 997	–	1 fixed 10/100 port
Cisco 585 LRE CPE	–	4 fixed 10/100 ports

Table 2 Other Hardware Supported (continued)

Hardware	Software Image	Description
GBIC modules	–	• 1000BASE-SX GBIC • 1000BASE-LX/LH GBIC • 1000BASE-ZX GBIC • 1000BASE-T GBIC (model WS-5483) • CWDM[2] fiber-optic GBIC[3] • DWDM[4] fiber-optic GBIC • GigaStack GBIC
Redundant power system	–	• Cisco RPS 300 redundant power system • Cisco RPS 675 redundant power system
SFP devices	–	• 1000BASE-SX SFP module • 1000BASE-LX\LH SFP module • 1000BASE-ZX SFP module • 1000BASE-T SFP module • CWDM

1. CPE = customer premises equipment
2. CDWM = coarse wavelength-division multiplexing
3. This feature is only supported when your switch is running the EI.
4. DWDM = dense wavelength-division multiplexing

Hardware Not Supported

Table 3 lists the hardware that is not supported by this release.

Table 3 Hardware Not Supported

Hardware	Description
GBIC module	1000BASE-T GBIC (model WS-G4582)
Redundant power system	Cisco RPS 600 Redundant Power System

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 5

Hardware Requirements

Table 4 lists the minimum hardware requirements for running the device manager.

Table 4 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 5 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 5 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Netscape Navigator
Windows 98	None	5.5 or 6.0	7.1
Windows NT 4.0	Service Pack 6 or later	5.5 or 6.0	7.1
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 that has the latest software should be the command switch, unless your command switch is running Cisco IOS Release 12.1(19)EA1 or later.
- 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, and the command reference.

CNA Compatibility

Cisco IOS 12.1(11)EA7 and later are only compatible with Cisco Network Assistant (CNA) 3.1 and later. You can download CNA 3.1 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

Before downloading software, read this section for important information. This section describes these procedures for downloading software:

- "Finding the Software Version and Feature Set" section on page 7
- "Deciding Which Files to Download from Cisco.com" section on page 7
- "Archiving Software Images" section on page 8
- "Upgrading a Switch by Using the Device Manager or Network Assistant" section on page 9
- "Upgrading a Switch by Using the CLI" section on page 9
- "Recovering from Software Failure" section on page 14

For information about the software releases that support the switches, see the "Catalyst 2950 Hardware and Software Compatibility Matrixes" section on page 24.

Note The Catalyst 2950-12 and Catalyst 2950-24 switches cannot be upgraded to Cisco IOS Release 12.1(6)EA2, Cisco IOS Release 12.1(6)EA2a, or Cisco IOS Release 12.1(6)EA2b. They can be upgraded to Cisco IOS Release 12.1(6)EA2c or later.

When you upgrade a switch, the switch continues to operate while the new software is copied to flash memory. If flash memory has enough space, the new image is copied to the selected switch but does not replace the running image until you reboot the switch. If a failure occurs during the copy process, you can still reboot your switch by using the old image. If flash memory does not have enough space for two images, the new image is copied over the existing one. Features provided by the new software are not available until you reload the switch.

If a failure occurs while copying a new image to the switch, and the old image has already been deleted, see the "Recovering from Corrupted Software" section in the "Troubleshooting" chapter of the software configuration guide for this release.

For information about upgrading the LRE switch firmware, see the "Upgrading LRE Switch Firmware" section in the software configuration guide for this release.

Caution A bootloader upgrade occurs if you are upgrading Catalyst 2950 switches running Cisco IOS Release 12.1(9)EA1d or earlier to Cisco IOS Release 12.1(11)EA1 or later for both cryptographic and noncryptographic images.
When you first upgrade the switch from a Cisco IOS noncryptographic image to a cryptographic image, the bootloader automatically upgrades. The new bootloader upgrade can take up to 30 seconds. Do not

power cycle the switch the first time that you are upgrading the switch to a cryptographic Cisco IOS image. If a power failure occurs when you are copying this image to the switch, call Cisco Systems immediately.

Caution Do not power cycle the switch while you are copying an image to the switch. If a power failure occurs while you are copying the software image to the switch, and there are no other images on the switch, see the "Troubleshooting" chapter in the software configuration guide for detailed recovery procedures.

Finding the Software Version and Feature Set

The 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** user EXEC command to see the software version that is running on your switch. In the display, check the line that begins with `System image file is`. This line shows the directory name in flash memory where the image is stored. A couple of lines below the image name, you see `Running Enhanced Image` if you are running the EI or `Running Standard Image` if you are running the SI.

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 Download from Cisco.com

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains both the Cisco IOS image file and the embedded device manager files. You must use the combined tar file to upgrade the switch through the device manager.

The tar file is an archive file from which you can extract files by using the **archive tar** command.

Note If you are upgrading a non-LRE Catalyst 2950 switch from a release earlier than Cisco IOS Release 12.1(6)EA2, use the **tar** command instead of the **archive tar** command.

Table 6 lists the software filenames for this release. These files are posted on Cisco.com.

Table 6 Catalyst 2955, 2950, and Catalyst 2940 Cisco IOS Software Files

Filename	Description
c2955-i6k2l2q4-tar.121-22.EA7.tar	Catalyst 2955 EI files. This includes the cryptographic Cisco IOS image and the device manager files.
c2955-i6q4l2-tar.121-22.EA7.tar	Catalyst 2955 EI files. This includes the Cisco IOS image and the device manager files.
c2950-i6k2l2q4-tar.121-22.EA7.tar	Catalyst 2950 SI[1] and EI files. This includes the cryptographic Cisco IOS image and the device manager files.

Table 6 Catalyst 2955, 2950, and Catalyst 2940 Cisco IOS Software Files (continued)

Filename	Description
c2950-i6q4l2-tar.121-22.EA7.tar	Catalyst 2950 SI and EI files. This includes the Cisco IOS image and the device manager files.
c2950lre-i6k2l2q4-tar.121-22.EA7.tar	Catalyst 2950 LRE EI files. This includes the cryptographic Cisco IOS image and the device manager files.
c2950lre-i6l2q4-tar.121-22.EA7.tar	Catalyst 2950 LRE EI files. This includes the Cisco IOS image and the device manager files.
c2940-i6k2l2q4-tar.121-22.EA7.tar	Catalyst 2940 files. This includes the cryptographic Cisco IOS image and the device manager files.
c2940-i6q4l2-tar.121-22.EA7.tar	Catalyst 2940 files. This includes the Cisco IOS image and the device manager files.

1. Switches that support only the SI cannot run the cryptographic image. For more information, see the SI-only switches listed in Table 1 and the "Cisco IOS Limitations and Restrictions" section on page 15.

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/partner/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 "Additional File Transfer Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.1* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frprt2/frd2006.htm#1018426

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. From the feature bar, choose **Administration > Software Upgrade**. 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

To upgrade the switch software by using the CLI, see Table 6 to decide which software files that you need, and then follow these procedures in this order:

1. Download the tar files from Cisco.com, as described in the "Downloading the Software" section on page 9.
2. Copy the current startup configuration file, as described in the "Copying the Current Startup Configuration from the Switch to TFTP Server" section on page 10.
3. Use the CLI to extract the image and the device manager files from the tar file:
   - If your switch is a Catalyst 2950 LRE or Catalyst 2940 switch, see the "Using the CLI to Upgrade a Catalyst 2950 LRE or Catalyst 2940 Switch" section on page 10.
   - If your switch is a Catalyst 2955 or non-LRE Catalyst 2950, switch, see the "Using the CLI to Upgrade a Catalyst 2955 Switch or Non-LRE Catalyst 2950 Switch" section on page 12.

Downloading the Software

This procedure is for copying the combined tar file to a 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.

Follow these steps to download the software from Cisco.com to your management station:

Step 1 Download the files from one of these locations:

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 files, click the link for your switch platform, and then follow the links on the page to select the correct tar image file.

Step 2 Use the CLI or web-based interface to perform a TFTP transfer of the file or files to the switch after you have downloaded them to your PC or workstation.

New features provided by the software are not available until you reload the software.

Copying the Current Startup Configuration from the Switch to TFTP Server

When you make changes to a switch configuration, your changes become part of the running configuration. When you enter the command to save those changes to the startup configuration, the switch copies the configuration to the config.text file in flash memory. To ensure that you can recreate the configuration if a switch fails, you might want to copy the config.text file from the switch to a TFTP server.

Beginning in privileged EXEC mode, follow these steps to copy a switch configuration file to the TFTP server.

Step 1 Copy the file in flash memory to the root directory of the TFTP server:

```
switch# copy flash:config.text tftp
```

Step 2 Enter the IP address of the device where the TFTP server resides:

```
Address or name of remote host []? ip_address
```

Step 3 Enter the name of the destination file (for example, **config.text**):

```
Destination filename [config.text]? yes/no
```

Step 4 Verify the copy by displaying the contents of the root directory on the TFTP server.

Using the CLI to Upgrade a Catalyst 2950 LRE or Catalyst 2940 Switch

Use this procedure for upgrading your Catalyst 2950 LRE or Catalyst 2940 switch by using the **archive download-sw** privileged EXEC command to automatically extract and download the Cisco IOS image and the device manager files to the switch. The **archive download-sw** command initiates this process:

- It verifies adequate space on the flash memory before downloading the new set of images.
- If there is insufficient space on the flash memory to hold both the old and the new images, it deletes the old set of images. The images are always stored in a subdirectory on the flash memory. The subdirectory name is the same as the image release name, for example, *flash:/c2940-i6q412-tar.121.22.EA5/*
- It replaces the old set of images with the new set of images. The set includes the Cisco IOS image and the device manager files and, on Catalyst 2950 LRE switches, the LRE firmware files. You do not have to manually delete the device manager directory from flash memory.
- After the new set of files is downloaded, it automatically sets the BOOT environment variable.
- If you enter the command with the **/reload** or the **/force-reload** option, it automatically reloads the switch after the upgrade.

For further information on this command, see the command reference for this release.

Follow these steps to upgrade the switch software by using a TFTP transfer:

Step 1 If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

Step 2 Log into the switch by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter this command:

```
server% telnet switch_ip_address
```

Enter the Telnet password if you are prompted to do so.

Step 3 Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

Step 4 Ensure that you have IP connectivity to the TFTP server by using 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 5 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 using this privileged EXEC command:

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.

Note You must use the /**overwrite** option when upgrading a Catalyst 2940 switch.

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/c2940-i612-tar.121-22.EA5.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.

Your Telnet session ends when the switch reloads.

After the switch reboots, use Telnet to return to the switch, and enter the **show version** user EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and start it again to ensure that you are using the latest HTML files.

Using the CLI to Upgrade a Catalyst 2955 Switch or Non-LRE Catalyst 2950 Switch

Use this procedure for upgrading your Catalyst 2955 or non-LRE Catalyst 2950 switch by copying the tar file to the switch. You copy the Cisco IOS image and the device manager files to the switch from a TFTP server and then extract the files by entering the **archive tar** command, with these results:

- Changes the name of the current image file to the name of the new file that you are copying and replaces the old image file with the new one. Perform this step only if you have space available on your switch.
- Disables access to the device manager pages and deletes the existing device manager files before the software upgrade to avoid a conflict if users access the web pages during the software upgrade.
- Re-enables access to the device manager pages after the upgrade is complete.

Caution A bootloader upgrade occurs if you are upgrading Catalyst 2950 switches running Cisco IOS Release 12.1(9)EA1d or earlier to Cisco IOS Release 12.1(11)EA1 or later for both cryptographic and noncryptographic images.
When you first upgrade the switch from a Cisco IOS noncryptographic image to a cryptographic image, the bootloader automatically upgrades. The new bootloader upgrade can take up to 30 seconds. Do not power cycle the switch the first time that you are upgrading the switch to a cryptographic Cisco IOS image. If a power failure occurs when you are copying this image to the switch, call Cisco Systems immediately.

Before downloading the new image, use the **dir** user EXEC command to confirm that you have enough space on the flash. The new image and HTML files will be slightly larger than the size of the tar file.

If you do not have enough space on the flash for the tar file, delete any old unused Cisco IOS images. If that does not free up enough flash space, delete the HTML files.

Caution Do not delete the image that you are currently running on the switch. If the switch fails while downloading the new image, you will need to use this.Follow these steps to upgrade the switch software by using a TFTP transfer:

Step 1 If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

Step 2 Log into the switch by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter this command:

```
server% telnet switch_ip_address
```

Enter the Telnet password if you are prompted to do so.

Step 3 Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

Step 4 Remove the switch HTML files:

```
switch# delete /r /f flash:html
```

where **/r** is for /recursive and **/f** is for /force. This command deletes all the switch HTML files and subdirectories.

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.

Step 5 Enter this command to copy the new image and the device manager files to flash memory:

Caution In this step, the **archive tar** command copies the tar file that contains both the image and the device manager files. If you are upgrading from a release earlier than Cisco IOS Release 12.1(6)EA2, use the **tar** command instead of the **archive tar** command.

```
switch# archive tar /x tftp://server_ip_address/path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!)
extracting info (110 bytes)
extracting c2950-i6q4l2-mz.121-13.EA1c.bin (2239579 bytes)!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)
extracting html/GraphFrame.html.gz (802 bytes)!
...
```

Depending on the TFTP server being used, you might need to enter only one slash (/) after the *server_ip_address* in the **archive tar** command.

Step 6 Display the name of the running (default) image file (BOOT path-list). This example shows the name in italic:

```
switch# show boot
BOOT path-list:    flash:current_image
Config file:       flash:config.text
Enable Break:      1
Manual Boot:       no
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

Step 7 Enter global configuration mode:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 8 Enter the **boot** command with the name of the new image filename:

```
switch(config)# boot system flash:new_image
```

For example:

```
switch(config)# boot system flash:c2950-i6q4l2-mz.121-13.EA1c.bin
```

Note If the **show boot** command entered in Step 6 displays no image name, you do not need to enter this command; the switch automatically finds the correct file to use when it resets.

Step 9 Return to privileged EXEC mode:

```
switch(config)# end
```

Step 10 Reload the new software with this command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

Step 11 Press **Return** to confirm the reload.

Your Telnet session ends when the switch reloads.

After the switch reboots, use Telnet to return to the switch, and enter the **show version** user EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and start it again to ensure that you are using the latest device manager files.

Recovering from Software Failure

If the software fails, you can reload the software. For detailed recovery procedures, see the "Troubleshooting" chapter in the software configuration guide for your switch.

Installation Notes

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

- The Express Setup program on Catalyst 2950 (including Catalyst 2950 LRE switches) and Catalyst 2940 switches. The Express Setup program is not supported on Catalyst 2955 switches.

  For more information about Express Setup, see the "Quick Setup" chapter in the Catalyst 2950 and Catalyst 2940 getting started guides.
- The CLI-based setup program.

  This procedure is described in the Catalyst 2955, Catalyst 2950, and Catalyst 2940 hardware installation guides.
- The DHCP-based autoconfiguration. See the software configuration guide for your switch.
- Manually assigning an IP address. See the software configuration guide for your switch.

New Features

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

- "New Hardware Features" section on page 14
- "New Software Features" section on page 15

New Hardware Features

For a complete list of supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

This release contains these new switch enhancements:

- DHCP for automating configuration of switch information (such as IP address, default gateway, host name, and Domain Name System [DNS] and TFTP server names). (Catalyst 2940 switches only)
- DHCP relay agent information (option 82) for subscriber identification and IP address management. (Catalyst 2940 switches only)
- Preconfigure a switch using Auto-Install and a saved configuration file before deploying the switch on the network. (Catalyst 2940 switches only)
- Support for up to 128 VLANs. (Catalyst 2940 switches and Catalyst 2950 switches running the SI)
- DHCP-base autoconfiguration automatically configures a switch at startup with IP address information and a configuration file. (Catalyst 2940 switches only)
- IEEE 802.1x with restricted VLAN to provide limited services to users who are IEEE 802.1x-compliant, but do not have the credentials to authenticate through the standard IEEE 802.1x processes.
- Support for the CISCO-PORT-QOS-MIB. (Catalyst 2940 switches only)
- Support for the **mac address-table static drop** global configuration command on the SI image.

Limitations and Restrictions

You should review this section before you begin working with the switches. 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.

Note These limitations and restrictions apply to all Catalyst 2955, Catalyst 2950, and Catalyst 2940 switches unless otherwise noted.

These sections describe the limitations and restrictions:

- "Cisco IOS Limitations and Restrictions" section on page 15
- "LRE Limitations and Restrictions" section on page 22
- "Device Manager Limitations and Restriction" section on page 24
- "Catalyst 2950 Hardware and Software Compatibility Matrixes" section on page 24

Cisco IOS Limitations and Restrictions

These limitations and restrictions apply to the Cisco IOS configuration:

- Root guard is inconsistent when configured on a port that is in the STP blocked state at the time of configuration. (CSCdp85954)
- Aging of dynamic addresses does not always occur exactly after the specified aging time elapses. It might take up to three times this time period before the entries are removed from the table. (CSCdr96565)

- Internal loopback in half-duplex mode causes input errors. We recommend that you configure the PHY to operate in full duplex before setting the internal loopback. (CSCds20365)
- If the switch gets configured from the dynamic IP pool, a duplicate or different IP address might be assigned.

  The workaround is to make sure that the DHCP server contains reserved addresses that are bound to each switch by the switch hardware address so that the switch does not get its IP address from the dynamic pool. (CSCds58369)
- A source-based distribution port group does not share the broadcast with all the group members. When the destination of the packets is a broadcast or unknown unicast or multicast, the packets are forwarded only on one port member of a port group, instead of being shared among all members of the port group. (CSCdt24814)
- When you enter the **show controllers ethernet-controller** *interface-id* or **show interfaces** *interface-id* **counters** privileged EXEC command, if a large number of erroneous frames are received on an interface, the receive-error counts might be smaller than the actual values, and the receive-unicast frame count might be larger than the actual frame count. (CSCdt27223)
- Two problems occur when a switch is in transparent mode:
  - If the switch is a leaf switch, any new VLANs added to it are not propagated upstream through VTP messages. As a result, the switch does not receive flooded traffic for that VLAN.
  - If the switch is connected to two VTP servers, it forwards their pruning messages. If the switch has a port on a VLAN that is not requested by other servers through their pruning messages, it does not receive flooded traffic for that VLAN.

  There is no workaround. (CSCdt48011)
- The receive count output for the **show controllers ethernet-controller** *interface-id* privileged EXEC command shows the incoming packets count before the ASIC makes a decision of whether to drop the packet or not. Therefore, for ports in the STP blocking states, even though the receive count shows incoming frames, the packet is not forwarded to the other port. (CSCdu83640)
- In some network topologies, when UplinkFast is enabled on all switches and BackboneFast is not enabled on all switches, a temporary loop might be caused when the STP root switch is changed.

  The workaround is to enable BackboneFast on all switches. (CSCdv02941)
- At times, the Window XP pop-up window might not appear while authenticating a client (supplicant) because the user information is already stored in Windows XP. However, the Extensible Authentication Protocol over LAN (EAPOL) response to the switch (authenticator) might have an empty user ID that causes the IEEE 802.1x port to be unauthenticated.

  The workaround is to manually re-initiate authentication by either logging off or detaching the link and then reconnecting it. (CSCdv19671)
- If two Catalyst 2950 switches are used in a network and if access ports are used to connect two different VLANs whose VLAN IDs are separated by the correct multiple of 64, it is possible to create a situation where the two switches use the same bridge ID in the same spanning-tree instances. This might cause a loss of connectivity in the VLAN as the spanning tree blocks the ports that should be forwarding.

  The workaround is to not cross-connect VLANs. For example, do not use an access port to connect VLAN 1 to VLAN 65 on either the same switch or from one switch to another switch. (CSCdv27247)

- A command switch might not show the Catalyst 1900, Catalyst 2820, and Catalyst 2900 XL 4-MB (models C2908-XL, C2916M-XL, C2924C-XL, and C2924-XL) switches as candidates even though their management VLAN is the same as the command switch. This occurs only when their management VLAN is not VLAN 1. (CSCdv34505)
- You can configure up to 256 Multicast VLAN Registration (MVR) groups by using the **mvr vlan group** interface configuration command, but only 255 groups are supported on a Catalyst 2950 switch at one time. If you statically add a 256th group, and 255 groups are already configured on the switch, it continues trying (and failing) to add the new group.

  The workaround is to set the mode to **dynamic** for Catalyst 2950 switches that are connected to IGMP-capable devices. The new group can join the multicast stream if another stream is dynamically removed from the group. (CSCdv45190)
- A Catalyst 2950 command switch can discover only the first Catalyst 3550 switch if the link between the Catalyst 3550 switches is an IEEE 802.1Q trunk and the native VLAN is not the same as the management VLAN of the Catalyst 2950 switch or if the link between the Catalyst 3550 switches is an Inter-Switch Link (ISL) trunk and the management VLAN is not VLAN 1.

  The workaround is to connect Catalyst 3550 switches by using the access link on the command switches management VLAN or to configure an IEEE 802.1Q trunk with a native VLAN that is the same as the management VLAN of the command switch. (CSCdv49871)
- There might be a link on the Fast Ethernet port of the Catalyst 2950 switch when it is forced to 10 Mbps and full-duplex mode and its link partner is forced to 100 Mbps and forced duplex mode. The LED on the Catalyst 2950 switch might display the link, and the error counters might increment.

  The workaround is to configure both sides of a link to the same speed or use autonegotiation. (CSCdv62271)
- The **ip http authentication enable** global configuration command is not saved to the configuration file because this is the default configuration. Therefore, this configuration is lost after a reboot.

  The workaround is to manually enter the command again after a reboot. (CSCdv67047)
- If a stack that has Catalyst 2955, Catalyst 2950, or Catalyst 2940 switches also has Catalyst 2900 XL *or* Catalyst 3500 XL switches, cross-stack UplinkFast (CSUF) does not function if the management VLAN on the Catalyst 2900 XL or Catalyst 3500 XL switches is changed to a VLAN other than VLAN 1 (the default).

  The workaround is to make sure that the management VLANs of all Catalyst 2900 XL or 3500 XL switches in the stack are set to VLAN 1. (CSCdv82224)
- If a port is configured as a secure port with the violation mode as restrict, the secure ports might process packets even after maximum limit of MAC addresses is reached, but those packets are not forwarded to other ports. (CSCdw02638)
- The *discarded frames* count of the **show controllers ethernet-controller** privileged EXEC command output and the *ignored* count of the **show controller ethernet** privileged EXEC command output can increment for these reasons:
  - The source and destination ports are the same.
  - The spanning-tree state of the ingress port is not in the forwarding state.
  - Traffic is filtered because of unicast or multicast storms are on the port.
  - Traffic is dropped because a VLAN has not been assigned by VLAN Query Protocol (VQP).

Note This error occurs only on switches that can run Cisco IOS Release 12.0(5)WC2b or earlier.

There is no workaround. (CSCdw48441)

- You can apply ACLs to a management VLAN or to any traffic that is going directly to the CPU, such as SNMP, Telnet, or web traffic. For information on creating ACLs for these interfaces, see the "Configuring IP Services" section of the *Cisco IOS IP and IP Routing Configuration Guide for Cisco IOS Release 12.1* and the *Cisco IOS IP and IP Routing Command Reference for Cisco IOS Release 12.1*.
- The SSH feature uses a large amount of switch memory, which limits the number of VLANs, trunk ports, and cluster members that you can configure on the switch. Before you download the cryptographic software image, your switch configuration must meet these conditions:
  - The number of trunk ports multiplied by the number of VLANs on the switch must be less than or equal to 128. These are examples of switch configurations that meet this condition:

    If the switch has 2 trunk ports, it can have up to 64 VLANs.

    If the switch has 32 VLANs, it can have up to 4 trunk ports.
  - If your switch is a cluster command switch, it can only support up to eight cluster members.

Note A switch that runs the SI cannot run the cryptographic image. If a cryptographic image is loaded on an SI-only switch, the switch will perform a forced reload.

If your switch has a saved configuration that does not meet the previous conditions and you upgrade the switch software to the cryptographic software image, the switch might run out of memory. If this happens, the switch does not operate properly. For example, it might continuously reload.

If the switch runs out of memory, this message appears:

```
%SYS-2-MALLOCFAIL: Memory allocation of (number_of_bytes) bytes failed ...
```

The workaround is to check your switch configuration and ensure that it meets the previous conditions. (CSCdw66805)

- When you use the **policy-map** global configuration command to create a policy map, and you do not specify any action for a class map, the association between that class map and policy map is not saved when you exit **policy-map** configuration mode.

  The workaround is to specify an action in the policy map. (CSCdx75308)
- When a community string is assigned by the cluster command switch, you cannot get any dot1dBridge MIB objects by using a community string with a VLAN entity from a cluster member switch.

  The workaround is to manually add the cluster community string with the VLAN entity on the member switches for all active VLANs shown in the **show spanning-tree summary** display. This is an example of such a change, where *cluster member 3* has spanning tree on *vlan 1-3*, and the cluster commander community string is *public@es3*.

```
Switch(config)# snmp community public@es3@1 RO
Switch(config)# snmp community public@es3@2 RO
Switch(config)# snmp community public@es3@3 RO
```

  There is no workaround. (CSCdx95501)

- When the Internet Group Management Protocol (IGMP) Immediate Leave is configured, new ports are added to the group membership each time a join message is received, and ports are pruned (removed) each time a leave message is received.

  If the join and leave messages arrive at high rate, the CPU can become busy processing these messages. For example, the CPU usage is approximately 50 percent when 50 pairs of join and leave messages are received each second. Depending on the rate at which join and leave messages are received, the CPU usage can go very high, even up to 100 percent, as the switch continues processing these messages.

  The workaround is to only use the Immediate Leave processing feature on VLANs where a single host is connected to each port. (CSCdx95638)

- A switch does not use the default gateway address in the DHCP offer packet from the server during automatic-install process.

  The workaround is to manually assign an IP address to the switch. (CSCdy08716)

- In a Remote Switched Port Analyzer (RSPAN) session, if at least one switch is used as an intermediate or destination switch *and* if traffic for a port is monitored in both directions, traffic does not reach the destination switch.

  These are the workarounds:

  – Use a Catalyst 3550 or Catalyst 6000 switch as an intermediate or destination switch.

  – Monitor traffic in only one direction if a Catalyst 2950 switch is used as an intermediate or destination switch. (CSCdy38476)

- If you assign a nonexistent VLAN ID to a static-access EtherChannel by setting the ciscoVlanMembershipMIB:vmVlan object, the switch does not create the VLAN in the VLAN database. (CSCdy65850)

- When you configure a dynamic switch port by using the **switchport access vlan dynamic** interface configuration command, the port might allow unauthorized users to access network resources if the interface changes from access mode to trunk mode through Dynamic Trunking Protocol (DTP) negotiation.

  The workaround is to configure the port as a static access port. (CSCdz32556)

- The output from the **show stack** privileged EXEC command might show a large number of false interrupts.

  There is no workaround. The number of interrupts does not affect the switch functionality. (CSCdz34545)

- If you configure a static secure MAC address on an interface before enabling port security on the interface, the same MAC address is allowed on multiple interfaces. If the same MAC address is added on multiple ports before enabling port security and port security is later enabled on those ports, only the first MAC address can be added to the hardware database. If port security is first enabled on the interface, the same static MAC address is not allowed on multiple interfaces. (CSCdz74685)

- In Cisco IOS Release 12.1(13)EA1 or later, these are the default settings for a IP Phone connected to a switch:

  – The port trust state is to not trust the priority of frames arriving on the IP Phone port from connected devices.

  – The class of service (CoS) value of incoming traffic is overwritten and set to zero. (CSCdz76915)

- If you press and hold the spacebar while the output of any **show** user EXEC command is being displayed, the Telnet session is stopped, and you can no longer communicate with the management VLAN.

  These are the workarounds:

  – Enter the show commands from privileged EXEC mode, and use this command to set the terminal length to zero:

  ```
  switch# terminal length 0
  ```

  – Open a Telnet session directly from a PC or workstation to the switch.

  – Do not hold down the spacebar while scrolling through the output of a **show** user EXEC command. Instead, slowly press and release the spacebar. (CSCea12888)

- When you connect a switch to another switch through a trunk port and the number of VLANs on the first switch is lower than the number on the connected switch, interface errors are received on the management VLAN of the first switch.

  The workaround is to match the configured VLANs on each side of the trunk port. (CSCea23138)

- When you enable Port Fast on a static-access port and then change the port to dynamic, Port Fast remains enabled. However, if you change the port back to static, Port Fast is disabled.

  The workaround is to configure Port Fast globally by using the **spanning-tree portfast** global configuration command. (CSCea24969)

- When using the SPAN feature, the monitoring port receives copies of sent and received traffic for all monitored ports. If the monitoring port is oversubscribed, it will probably become congested. This might also affect how one or more of the monitored ports forwards traffic.

- When a 10/100 switch port is connected to a 10/00 port on a hub and another 10/100 port on the hub is connected to a 10/100 port on another switch, when one of the switches restarts, the link state might change from down to up, and these messages might appear:

  ```
  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
  %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
  ```

  Then the switch that restarted does not forward traffic until the spanning-tree state enters the forwarding state. This can occur on a switch running Cisco IOS Release 12.1(13)EA1 or later. (CSCea47230)

- On a Catalyst 2940 switch, when a 1000BASE-T SFP module is inserted in the SFP module slot, the output of the **show interface capabilities** privileged EXEC command incorrectly shows that the interface supports 10 Mbps, 100 Mbps, and 1000 Mbps. The SFP module supports only 1000 Mbps. (CSCeb31239)

- After a topology change in STP, some terminals connected to the management VLAN can transfer data because the affected switch ports start forwarding before they move to the forwarding state.

Note If the terminal does not belong to management VLAN, this failure does not occur.

  The workaround is to place the ports in static-access mode for a single VLAN, if the topology supports this configuration. (CSCec13986)

- (Catalyst 2950 switches) If a policy map is applied to a switch, it might be only partially applied on these ingress ports; Fast Ethernet 0/8, Fast Ethernet 0/16, Fast Ethernet 0/24, Fast Ethernet 0/32, Fast Ethernet 0/40, or Fast Ethernet 0/48.

  This problem occurs when:

  – All eight ports of a port group are configured to trust Differentiated Services Code Point (DSCP). A port group can have Fast Ethernet ports 1 to 8, 9 to 16, and so on.

  – A policy map is applied.

  – A port group has 75 or more access control entries (ACEs).

  The workaround is to use fewer than 75 ACEs per port group when configuring the ports to trust DSCP. (CSCed11617)

- 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 seen 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)

- If a switch receives STP packets and non-STP packets that have a CoS value of 6 or 7 and all of these packets belong to the same management VLAN, a loop might occur.

  These are the workarounds:

  – Change the CoS value of the non-STP packets to a value other than 6 or 7.

  – If the CoS value of the non-STP packets must be 6 or 7, configure these packets to belong to a VLAN other than the management VLAN. (CSCed88622)

- This problem can affect switches running Cisco IOS Release 12.1(22)EA4. The EtherChannel between two switches flaps, and this message appears:

  ```
  ERROR interrupt: PCI Fatal Error on DMA CH0
  ```

  This problem occurs when there is an EtherChannel between two switches, traffic is sent between the switches, and the RSPAN or SPAN source port is configured to monitor sent traffic.

  The workaround is to stop the SPAN traffic, and then delete and recreate the VLAN. (CSCeh20389)

- Certain combinations of features and switches create conflicts with the port security feature. In Table 7, *No* means that port security cannot be enabled on a port on the referenced switch if the referenced feature is also running on the same port. *Yes* means that both port security and the referenced feature can be enabled on the same port on a switch at the same time. A dash means not applicable.

Table 7 Port Security Incompatibility with Other Switch Features

Feature	Catalyst 2940	Catalyst 2950 and Catalyst 2955
DTP[1] port[2]	No	No
Trunk port	No	No
Dynamic-access port[3]	No	No
SPAN source port	Yes	Yes
SPAN destination port	No	No
EtherChannel	No	No

Table 7 Port Security Incompatibility with Other Switch Features (continued)

Feature	Catalyst 2940	Catalyst 2950 and Catalyst 2955
Protected port	Yes	Yes
IEEE 802.1x port	–	Yes[4]
Voice VLAN port[5]	Yes	Yes

1. DTP = Dynamic Trunking Protocol
2. A port configured with the **switchport mode dynamic** interface configuration command.
3. A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.
4. The switch must be running the enhanced software image (EI).
5. You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.

LRE Limitations and Restrictions

These limitations and restrictions apply only to Catalyst 2950 LRE switches:

- VLAN-tagged packets from multiple VLANs with the same source MAC address that are received on different Cisco 585 LRE CPE Ethernet ports create a single MAC address entry (ingress port entry). Any network designed with the assumption that MAC addresses are maintained per VLAN does not work.

  There is no workaround. The Ethernet port on the Cisco 585 LRE CPE does not support VLANs. All the ports are assumed to be in the same VLAN. (CSCdx03708)

- Maximum-sized ISL frames (frames between 1537 and 1544 bytes) are discarded by the CPE device on ingress interfaces. Some chips and switches on the CPE device support a maximum frame size of 1536 bytes, which causes any maximum-sized ISL frames coming into the CPE from an end device or from an LRE switch to be discarded.

  There is no workaround. You must ensure that the network does not send ISL tagged frames of sizes between 1537 and 1544 bytes to an LRE switch. (CSCdx25940)

- The system runs out of memory and fails after too many RMON buckets are requested.

  There is no workaround; only 1000 buckets per interface are supported. (CSCdy38390)

- The flow control autonegotiation settles in the incorrect outcome if you use a Cisco-made 1000BASE-T GBIC with any switch not listed in Table 1 of the 1000BASE-T GBIC Switch Compatibility Matrix:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/1000gbic/1000comp.htm.

  The workaround is to use the Cisco 1000BASE-T GBIC only with compatible switches. (CSCdy53369)

- The flash memory write operation is slower on LRE switches than on non-LRE switches. (CSCdy55897)

- The Cisco 585 LRE CPE has four Fast Ethernet ports. When the CPE is connected to an LRE switch, the default value for the maximum number of secure MAC addresses is 1. You can use the **show port-security** command to display the current maximum value.

  The workaround is to use the **switchport port-security maximum** *value* interface configuration command to change the default value. For interfaces connected to Cisco 575 LRE and Cisco 576 LRE 997 CPEs, the default value can be 1. For interfaces connected to Cisco 585 LRE CPEs, the value can be 5 because the CPE has four Fast Ethernet ports and one additional MAC address. (CSCdy73748)

- The Cisco 575 LRE or the Cisco 576 LRE 997 CPE does not support all of the Fast Ethernet statistics displayed by the **show controllers ethernet-controller longreachethernet** *interface-id* **cpe** command. The Cisco 585 LRE CPE supports all the LRE and CPE Fast Ethernet statistics.

  There is no workaround. These CPE Fast Ethernet statistics are supported by the Cisco 575 LRE CPE and the Cisco 576 LRE 997 CPE (CSCdy89348):

```
1 Transmit receive 0 bytes
0 Bytes
0 Unicast frames
0 Broadcast frames
0 Pause frames
0 Alignment errors
0 One collision frames
0 Multiple collisions
0 Undersize frames
0 Late collisions
0 Oversize frames
0 Excess collisions
0 FCS errors
0 Deferred frames
```

- When the *entPhysicalTable* object is retrieved, the copper physical entry is not included.

  There is no workaround. (CSCdz06748)

- When an IEEE 802.1x protocol-enabled client attempts to connect to a Catalyst 2950 LRE switch through a Cisco 585 LRE CPE with IEEE 802.1x configured on a port, the client cannot be authenticated. This problem does not affect the Cisco 575 LRE CPE or the Cisco 576 LRE 997 CPE. The **show dot1x interface** *interface* configuration command displays the port state as unauthorized. (CSCdz22965)

- When a Fast Ethernet port on a Cisco 585 LRE CPE is in half-duplex mode and the rate at which the port receives packets is higher than rate at which it can forward packets, the *Pause Frames* counter for the CPE port increments.

  There is no workaround. (CSCea41362)

- On a Catalyst 2950 LRE switch running Cisco IOS Release 12.1(11)YJ4 or later, a Cisco 575 LRE CPE or a Cisco 576 LRE 997 CPE that does not have an LRE link but is connected to a remote device through the Ethernet link might see repeated flaps on the Ethernet link. This does not occur on a Cisco 585 LRE CPE. (CSCeb01097)

- When a Cisco Catalyst 2950 LRE running Cisco IOS 12.1(14)EA1 or Cisco IOS 12.1(11)YJ is connected to Cisco 575 LRE CPE, the Fast Ethernet link on the CPE port fails to activate if you change the CPE speed setting from 10 to 100 Mbps while the CPE duplex mode is set to half or full.

  The workaround is to reset the CPE port by using the **cpe shutdown** followed by the **no cpe shutdown** interface configuration command. This activates the Fast Ethernet link on the CPE port. (CSCeb35007)

- When you shut down the 100BASE-FX port on the Catalyst 2950 switch, the upstream switch does not detect loss of link, and the line protocol stays up.

  Configure UDLD aggressive mode (using the **udld port aggressive** interface configuration command) on both the Catalyst switch and neighboring device, and change the error- disable recovery options by using the **errdisable recovery cause udld** and **errdisable recovery interval 60** global configuration commands. (CSCee57059)

- On a Catalyst 2950 LRE switch running Cisco IOS Release 12.1(20)EA1 or later, the **flowcontrol** interface configuration commands only take effect when the LRE link comes up after being shut down.

  If the switch configuration is saved and the switch restarts, this does not affect the switch. However, if the flow control configuration for an LRE port is changed and the switch is not rebooted, the commands do not take effect unless you shut down and bring up the LRE link.

  The workaround is to enter the **shutdown** and **no shutdown** interface configuration commands on an interface after entering a **flowcontrol** interface configuration command, such as the **flowcontrol receive** or the **flowcontrol send** command. (CSCef26565)

Device Manager Limitations and Restriction

These device manager limitations and restrictions:

- This release supports the same switch cluster compatibilities supported in Cisco IOS Release 12.1(22)EA1. However, you cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or the Cisco Network Assistant application. For information about Network Assistant, see the "New Features" section on page 14.
- When you are prompted to accept the security certificate and you click *No*, you see only 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)

Catalyst 2950 Hardware and Software Compatibility Matrixes

Some Catalyst 2950 switches are not supported by certain software releases.

Table 8 lists the Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 switches and the software releases supporting them. The serial numbers are on the switch rear panel. In this table, *Yes* means that the switch is supported by the software release; *No* means that the switch is not supported by the release.

The Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, and 2950G-48-EI switches are supported by Cisco IOS Release 12.1(6)EA2 or later.

The Catalyst 2950SX-24 switches are supported by Cisco IOS Release 12.1(9)EA1d or later.

The Catalyst 2955 switches are supported by Cisco IOS Release 12.1(12c)EA1 or later.

The Catalyst 2950ST-8 LRE and 2950ST-24 LRE switches are supported by Cisco IOS Release 12.1(11)YJ or later.

The Catalyst 2950ST-24 LRE 997 switches are supported by Cisco IOS Release 12.1(11)YJ4 or later.

Table 8 Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches

Hardware	Serial Number	Cisco IOS Release 12.0(5)WC2b or Earlier	Cisco IOS Release 12.1(6)EA2, 12.1(6)EA2a, and 12.1(6)EA2b	Cisco IOS Release 12.1(6)EA2c	Cisco IOS Release 12.1(9)EA1 or Later
Catalyst 2950-12	Any serial number beginning with FAA or FAB	Yes	No	Yes	Yes
	Lower than FOC0616W1H6 or FHK0616W34M	Yes	No	Yes	Yes
	FOC0616W1H6, FHK0616W34M, or higher	No	No	Yes	Yes
Catalyst 2950-24	Any serial number beginning with FAA or FAB	Yes	No	Yes	Yes
	Lower than FOC0616Z1ZM or FHK0617Y0N3	Yes	No	Yes	Yes
	FOC0616Z1ZM, FHK0617Y0N3, or higher	No	No	Yes	Yes
Catalyst 2950C-24	Any serial number beginning with FAA or FAB	Yes	Yes	Yes	Yes
	Lower than FOC0616TOJH or FHK0617W0YA	Yes	Yes	Yes	Yes
	FOC0616TOJH, FHK0617W0YA, or higher	No	No	Yes	Yes
Catalyst 2950T-24	Any serial number beginning with FAA or FAB	Yes	Yes	Yes	Yes
	Lower than FOC0617X11P or FHK0617Y1M2	Yes	Yes	Yes	Yes
	FOC0617X11P, FHK0617Y1M2, or higher	No	No	Yes	Yes

The Cisco LRE CPE devices are not supported by certain Catalyst 2950 LRE switches. In Table 9, *Yes* means that the CPE is supported by the switch; *No* means that the CPE is not supported by the switch.

Table 9 LRE Switch and CPE Compatibility Matrix

LRE Devices	Catalyst 2950ST-8 LRE switch	Catalyst 2950ST-24 LRE switch	Catalyst 2950ST-24 LRE 997 switch
Cisco 575 LRE CPE	Yes	Yes	No
Cisco 576 LRE 997 CPE	No	No	Yes
Cisco 585 LRE CPE	Yes	Yes	No

Important Notes

Note These important notes apply to all Catalyst 2955, Catalyst 2950, and Catalyst 2940 switches unless otherwise noted.

This section describes important informations related to this release:

- "Cisco IOS Notes" section on page 26
- "Device Manager Notes" section on page 27

Cisco IOS Notes

These are the important Cisco IOS configuration notes related to this release:

- In Cisco IOS Release 12.1(14)EA1, the implementation for IEEE 802.1x changed from the previous release. Some global configuration commands became interface configuration commands, and new commands were added.

  If you have IEEE 802.1x configured on the switch and you upgrade to Cisco IOS Release 12.1(14)EA1 or later, the configuration file does not contain the new commands, and IEEE 802.1x does not operate. After the upgrade is complete, make sure to globally enable IEEE 802.1x by using the **dot1x system-auth-control** global configuration command. For more information, see the software configuration guide for this release.

- When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to 2 plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP Phone, the telephone requires up to two MAC addresses. The IP address of the phone is learned on the voice VLAN, and it might or might not be learned on the access VLAN. Connecting a PC to the Cisco IP phone requires additional MAC addresses.

- IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries.

- The **management** interface configuration command is not supported in Cisco IOS Release 12.1(6)EA2 or later. To shut down the current management VLAN interface and to enable the new management VLAN interface, use the **shutdown** and **no shutdown** interface configuration commands. See the *Catalyst 2950 and Catalyst 2955 Switch Command Reference* for information about using the **shutdown** interface configuration command.
- When an IEEE 802.1x-authenticated client is disconnected from an IP phone, hub, or switch and does not send an EAPOL-Logoff message, the switch interface does not change to the unauthorized state. If this happens, it can take up to 60 minutes for the interface to change to the unauthorized state when the re-authentication time is the default value (3600 seconds).

  The workaround is to change the number of seconds between re-authentication attempts by using the **dot1x timeout re-authperiod** *seconds* global configuration command. (CSCdz38483)
- The guest VLAN might not assign a DHCP address to some clients. This is a problem with the IEEE 802.1x client, not with the switch.

  The workaround is to either release and renew the IP address or to change the default timers. These examples show typical interface timer changes:

  ```
  dot1x timeout quiet-period 3
  dot1x timeout tx-period 5
  ```
- The **transmit-interface** *type number* interface configuration command is not supported.
- 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:

- 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** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, the default method of HTTP server user authentication. • **local**—Local user database, as defined on the Cisco router or access server. • **tacacs**—TACACS server.
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), 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, the default method of HTTP server user authentication. • **local**—Local user database, as defined on the Cisco router or access server. • **tacacs**—TACACS server.
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 that might cause possible unexpected activity in this software release.

- CSCeg09032

  Open Shortest Path First (OSPF) routes might not appear in the routing table after a topology change if Incremental SPF (iSPF) is enabled.

  The workaround is to disable iSPF.

- CSCsb79318

  if the re-authentication timer and re-authentication action is downloaded from the RADIUS server using the Session-Timeout and Termination-Action RADIUS attributes, the switch performs the termination action even when the port is not configured with the **dot1x timeout reauth server** global configuration command and uses the Termination-Action downloaded from a RADIUS server as part of IEEE 802.1x authorization.

  The workaround is to remove the Termination-Action attribute from the IEEE 802.1x policy on the RADIUS server if **dot1x timeout reauth server** is not configured on the port.

- CSCsb82422

  The switch does not forward an IEEE 802.1x request that has *null* credentials.

  There is no workaround.

- CSCsb93563

  When a Cisco IP phone is connected to the switch, the port VLAN ID (PVID) and the voice VLAN ID (VVID) both learn its MAC address. However, after dynamic MAC addresses are deleted, only VVID relearns the IP phone MAC address. MAC addresses are deleted manually or automatically for a topology change or when port security or an IEEE 802.1x feature is enabled or disabled.

  There is no workaround.

- CSCsb99249

  A host attached to an authenticated 802.1X port might not have network access after a 802.1X-enabled port mode or host mode is modified. This occurs when the 802.1X control direction is set to *In* when the configuration is changed.

  The workaround is to either shut down the 802.1X-enabled port or to remove the control-direction configuration before changing the port mode. You can do this by entering the **dot1x port-control**, **dot1x host-mode**, or **dot1x control-direction in** interface configuration commands.

- CSCsc96385

  The switch now sends the NAS-Identifier, attribute 32, to the RADIUS server when you configure the attribute in the running configuration by using these Cisco IOS global configuration commands:

  radius-server attribute 32 include-in-access-req [***format*** *%h*]

  r**adius-server attribute 32 include-in-accounting-req** [***format*** *&h*]

Resolved Caveats

Note All resolved caveats listed in these sections apply to the Catalyst 2955, Catalyst 2950, and Catalyst 2940 switches unless otherwise noted.

These are the Cisco IOS caveats resolved in this release:

- CSCsb53477

  When using Simple Network Management Protocol to disable the IEEE 802.1x guest VLAN feature, the SNMP client no longer receives an error message.

- CSCsb63404

  A switch is accessible by SSH or Telnet after it has been running for 4 to 5 days.

- CSCsb79517

  The Fast Ethernet port on a switch now will not lock up on transmit path under heavy management traffic.

Documentation Updates

Documentation Updates in Cisco IOS Release 12.1(22)EA7

These are the updates to the product documentation that occurred in Cisco IOS Release 12.1(22)EA7:

- Updates for the Software Configuration Guide, page 30
- Updates to the Command References, page 35

Updates for the Software Configuration Guide

Note The Catalyst 2940, 2950, and 2955 switches do not support IP IGMP `Querier`.

This information was added to the *Catalyst 2955 and 2950 Switch Software Configuration Guide*, Cisco IOS Release 12.1(22)EA2:

- VLAN Support, page 31
- Supported VLANs, page 31
- Normal-Range VLAN Configuration Guidelines, page 31
- Configuring Extended-Range VLANs, page 31
- IEEE 802.1x with Restricted VLAN, page 31
- Network Admission Control Layer 2 IEEE 802.1x Validation, page 34
- DHCP-Based Autoconfiguration with a Saved File, page 39

VLAN Support

This information was added to the "Overview" chapter of the *Catalyst 2955 and 2950 Switch Software Configuration Guide*:

Note The Catalyst 2950-12, Catalyst 2950-24, Catalyst 2950SX-24, Catalyst 2950SX-48-SI, and Catalyst 2950T-48-SI switches support only 128 port-based VLANs.

Supported VLANs

This information was added to the "Configuring VLANs" chapter of the *Catalyst 2955 and 2950 Switch Software Configuration Guide*:

Catalyst 2950 switches that run the standard software image (SI) support 128 VLANs; Catalyst 2940 switches support 128 VLANs.

Normal-Range VLAN Configuration Guidelines

The Catalyst 2940 switch supports a maximum of 128 VLANs.

Configuring Extended-Range VLANs

When the switch is in VTP transparent mode (VTP disabled), you can create extended-range VLANs (in the range 1006 to 4094 for any switch port commands that allow VLAN IDs).

This information was added to the "Configuring VTP" chapter of the *Catalyst 2955 and 2950 Switch Software Configuration Guide*:

VTP Modes

When the network is configured with more than the maximum 250 VLANs supported by the Catalyst 2950 switches running the enhanced software image (EI) or 128 VLANs supported by the Catalyst 2950 switches running the standard software image (SI), the switch automatically changes from VTP server or client mode to VTP transparent mode. The switch then operates with the VLAN configuration that preceded the one that sent it into transparent mode.

IEEE 802.1x with Restricted VLAN

This information was added to the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the *Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*, Cisco IOS Release 12.1(22)EA7:

- Using IEEE 802.1x with Restricted VLAN
- Configuring a Restricted VLAN

Using IEEE 802.1x with Restricted VLAN

You can configure a restricted VLAN for each IEEE 802.1x port on a switch to provide limited services to clients that cannot access the guest VLAN. These clients are IEEE 802.1x compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users without valid credentials in an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the restricted VLAN.

Note You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, the administrator can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator keeps a count of failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the restricted VLAN. The failed attempt count is incremented when RADIUS replies with either an *EAP failure* or an empty response that contains no EAP packet. When the port moves into the restricted VLAN, the failed attempt counter is reset.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves to either the configured VLAN or a VLAN sent by the RADIUS server. You can disable re-authentication. If you do this, the only way to start the authentication process again is for the port to receive a *link dow*n or *EAP logoff* event. We recommend that you keep re-authentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the *link down* or *EAP logoff* event.

After a port moves to the restricted VLAN, it sends a simulated EAP success message to the client, instead of an EAP failure message. This is done to prevent clients from attempting authentication indefinitely. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported only on IEEE 802.1x ports in single-host mode and on Layer 2 ports.

You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x restricted VLAN. The restricted VLAN feature is not supported on trunk ports; it is supported only on access ports.

This feature works with port security. As soon as the port is authorized, a MAC address is provided to port security. If port security does not permit the MAC address or if the maximum secure address count is reached, the port becomes unauthorized and error disabled.

Other port security features such as Dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the "IEEE 802.1x Configuration Guidelines" section on page 7-16.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**dot1x port-control auto**	Enable IEEE 802.1x authentication on the port.

	Command	Purpose
Step 5	**dot1x auth-fail vlan** *vlan-id*	Specify an active VLAN as an IEEE 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x restricted VLAN.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show dot1x interface** *interface-id*	(Optional) Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable and remove the restricted VLAN, use the **no dot1x auth-fail vlan** interface configuration command. The port returns to the unauthorized state.

This example shows how to enable VLAN 2 as an IEEE 802.1x restricted VLAN:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x auth-fail vlan 2
```

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the **dot1x auth-fail max-attempts** interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of allowed authentication attempts. This procedure is optional.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the "IEEE 802.1x Configuration Guidelines" section on page -3.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**dot1x port-control auto**	Enable IEEE 802.1x authentication on the port.
Step 5	**dot1x auth-fail vlan** *vlan-id*	Specify an active VLAN as an IEEE 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x restricted VLAN.
Step 6	**dot1x auth-fail max-attempts** *max attempts*	Specify a number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 3, and the default is 3.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show dot1x interface** *interface-id*	(Optional) Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default value, use the **no dot1x auth-fail max-attempts** interface configuration command.

This example shows how to set 2 as the number of authentication attempts allowed before the port moves to the restricted VLAN:

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```

Network Admission Control Layer 2 IEEE 802.1x Validation

This information about Nework Admission Control (NAC) Layer 2 IEEE 802.1x validation feature was added to the software configuration guide.

- This was added to the "Overview" chapter:

  Security Features

  NAC Layer 2 IEEE 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access.

- This information was added to the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the *Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*, Cisco IOS Release 12.1(20)EA2:

  Network Admission Control Layer 2 IEEE 802.1x Validation

  In Cisco IOS Release 12.1(22)EA6 and later, the switch supports the NAC Layer 2 IEEE 802.1x validation, which checks the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access. With NAC Layer 2 IEEE 802.1x validation, you can do these tasks:

  – Downloading the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) from the authentication server.

  – Setting the number of seconds between re-authentication attempts as the value of the Session-Timeout RADIUS attribute (Attribute[27]) and getting an access policy against the client from the RADIUS server.

  – Setting the action to be taken when the switch tries to re-authenticate the client by using the Termination-Action RADIUS attribute (Attribute[29]). If the value is the DEFAULT or is not set, the session ends. If the value is RADIUS-Request, the re-authentication process starts.

  – Viewing the NAC posture token, which shows the posture of the client, by using the **show dot1x** privileged EXEC command.

  – Configuring secondary private VLANs as guest VLANs.

  For information about configuring NAC Layer 2 IEEE 802.1x validation, see the "Configuring NAC Layer 2 IEEE 802.1x Validation" section on page 7-38 and the "Configuring Periodic Re-Authentication" section on page 7-27.

  For more information about NAC, see the *Network Admission Control Software Configuration Guide*.

  Configuring NAC Layer 2 IEEE 802.1x Validation

Beginning in privileged EXEC mode, follow these steps to configure NAC Layer 2 IEEE 802.1x validation. The procedure is optional.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**dot1x guest-vlan** *vlan-id*	Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x guest VLAN.

	Command	Purpose
Step 4	**dot1x reauthentication**	Enable periodic re-authentication of the client, which is disabled by default.
Step 5	**dot1x timeout reauth-period** {*seconds* | **server**}	Set the number of seconds between re-authentication attempts. The keywords have these meanings: • *seconds*—Sets the number of seconds from 1 to 65535; the default is 3600 seconds. • **server**—Sets the number of seconds based on the value of the Session-Timeout RADIUS attribute (Attribute[27]) and Termination-Action RADIUS attribute (Attribute [29]). This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show dot1x interface** *interface-id*	Verify your IEEE 802.1x authentication configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure NAC Layer 2 IEEE 802.1x validation:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
```

Supported MIBs

The Catalyst 2940 switches now support the CISCO-PORT-QOS-MIB. This MIB supports QoS statistics and per-port rate-limiting and traffic shaping.

Updates to the Command References

Note The Catalyst 2940, 2950, and 2955 switches do not support IP IGMP `Querier`.

These commands were added to the *Catalyst 2955 and 2950 Switch Command Reference, Cisco IOS Release 12.1(22)EA2*:

- dot1x auth-fail max-attempts, page 36
- dot1x auth-fail vlan, page 37
- show dot1x, page 38

dot1x auth-fail max-attempts

Use the **dot1x auth-fail max-attempts** interface configuration command to configure the maximum number of authentication attempts allowed before a port is moved to the restricted VLAN. To return to the default setting, use the **no** form of this command.

dot1x auth-fail max-attempts *max-attempts*

no dot1x auth-fail max-attempts

Syntax Description

max-attempts	Specify a maximum number of authentication attempts allowed before a port is moved to the restricted VLAN. The range is 1 to 3.

Defaults

The default is 3 attempts.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(22)EA7	This command was introduced.

Usage Guidelines

If you reconfigure the maximum number of authentication failures allowed by the VLAN, the change takes effect after the re-authentication timer expires.

Examples

This example shows how to set 2 as the maximum number of authentication attempts allowed before the port is moved to the restricted VLAN on Gigabit Ethernet interface 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x auth-fail max-attempts 2
Switch(config-if)# end
Switch(config)# end
Switch#
```

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

Related Commands

Command	Description
dot1x auth-fail vlan [*vlan id*]	Enables the optional restricted VLAN feature.
dot1x max-reauth-req [*count*]	Sets the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

dot1x auth-fail vlan

Use the **dot1x auth-fail vlan** interface configuration command to enable the restricted VLAN on a port. To return to the default setting, use the **no** form of this command.

dot1x auth-fail vlan *vlan-id*

no dot1x auth-fail vlan *vlan-id*

Syntax Description

vlan-id	Specify a VLAN in the range of 1 to 4094.

Defaults

No restricted VLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(22)EA7	This command was introduced.

Usage Guidelines

You can configure a restricted VLAN on ports configured as follows:

- single-host (default) mode only
- auto mode for authorization

You should enable re-authentication. The ports in restricted VLANs do not receive re-authentication requests if re-authentication is disabled. To start the re-authentication process, the restricted VLAN must receive a link down event or an Extensible Authentication Protocol (EAP) logoff event from the port. If the host is connected through a hub, the port might never receive a link down event and might not detect the new host until the next re-authentication attempt occurs. Therefore, re-authentication should be enabled.

If the user fails authentication, the port is moved to a restricted VLAN, and an EAP success message is sent to the user. Because the user is not notified of the authentication failure, there might be confusion as to why there is restricted access to the network. An EAP success message is sent for these reasons:

- If the EAP success message is not sent, the user tries to authenticate every 60 seconds (the default) by sending an EAP-start message.
- Some hosts (for example, devices running Windows XP) cannot implement DHCP until they receive an EAP success message.

A user might cache an incorrect username and password combination after receiving an EAP success message from the authenticator and re-use that information in every re-authentication. Until the user passes the correct username and password combination, the port remains in the restricted VLAN.

Internal VLANs that are used for Layer 3 ports cannot be configured as a restricted VLAN.

You cannot configure a VLAN to be both a restricted VLAN and a voice VLAN. If you do this, a syslog message is generated.

When a restricted VLAN port is moved to an unauthorized state, the authentication process is restarted. If the user fails the authentication process again, the authenticator waits in the held state. After the user has correctly re-authenticated, all IEEE 802.1x ports are reinitialized and treated as normal IEEE 802.1x ports.

When you reconfigure a restricted VLAN to a different VLAN, any ports in the restricted VLAN are also moved and the ports stay in their current authorized state.

When you shut down or remove a restricted VLAN from the VLAN database, any ports in the restricted VLAN are immediately moved to an unauthorized state and the authentication process is restarted. The authenticator does not wait in a held state because the restricted VLAN configuration still exists. While the restricted VLAN is inactive, all authentication attempts are counted. As soon as the restricted VLAN becomes active, the port is placed in the restricted VLAN.

The restricted VLAN is supported only in single-host mode (the default port mode).

When a port is placed in a restricted VLAN, the user's MAC address is added to the MAC address table. If a new MAC address appears on the port, it is treated as a security violation.

Examples

This example shows how to configure a restricted VLAN on Gigabit Ethernet interface 1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# end
Switch(config)# end
Switch#
```

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

Related Commands

Command	Description
dot1x auth-fail max-attempts [*max-attempts*]	Configures the number of authentication attempts allowed before assigning a user to the restricted VLAN.
show dot1x [**interface** *interface-id*]	Displays IEEE 802.1x status for the specified port.

show dot1x

The output for these commands changed:

This is an example of output from the **show dot1x all** privileged EXEC command when a restricted VLAN is configured:

```
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet0/1
----------------------------------------------------
Supplicant MAC 0002.b3eb.0df6
AuthSM State          = AUTHENTICATED(AUTH-FAIL-VLAN)
BendSM State          = IDLE
Posture               = N/A
PortStatus            = AUTHORIZED(AUTH-FAIL-VLAN)
MaxReq                = 2
MaxAuthReq            = 2
HostMode              = Single
PortControl           = Auto
ControlDirection      = Both
```

```
QuietPeriod           = 10 Seconds
Re-authentication     = Disabled
ReAuthPeriod          = 3600 Seconds
ServerTimeout         = 30 Seconds
SuppTimeout           = 30 Seconds
TxPeriod              = 10 Seconds
Guest-Vlan            = 3
AuthFail-Vlan         = 4
AuthFail-Max-Attempts = 3
```

This is an example of output from the **show dot1x interface fastethernet0/3** privileged EXEC command:

```
Switch# show dot1x interface fastethernet0/3
Supplicant MAC 00d0.b71b.35de
   AuthSM State      = AUTHENTICATED (AUTH-FAIL-VLAN)
   BendSM State      = IDLE
ReAuthPeriod = 4000 Seconds { (From Authentication Server) | (Locally Configured) }
ReAuthAction = { Terminate | Reauthenticate }
TimeToNextReauth = 1453 Seconds
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single (AUTH-FAIL-VLAN)
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

DHCP-Based Autoconfiguration with a Saved File

This information about DHCP-based autoconfiguration with a saved file feature was added to the software configuration guide.

- This was added to the "Overview" chapter:

  Ease of Use and Deployment Features

  DHCP-base autoconfiguration automatically configures a switch at startup with IP address

- This was added to the "Assigning the Switch IP Address and Default Gateway" chapter:

  Understanding DHCP-Based Autoconfiguration with a Saved Configuration File

  DHCP-based autoconfiguration with a saved configuration file works exactly the same as DHCP-based autoconfiguration except that you can now enable an autoconfiguration on a switch that already contains a basic configuration file in its memory.

  Configuring DHCP-Based Autoconfiguration with a Saved Configuration File

  Beginning in privileged EXEC mode, follow these steps to configure DHCP-based autoconfiguration with a saved configuration file:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**boot host dhcp**	Enable autoconfiguration with a saved configuration file.
Step 3	**boot host retry timeout** *timeout-value*	Set the amount of time between system retries.

	Command	Purpose
Step 4	**banner config-save ^C** *warning-message* **^C**	Create warning message.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show boot**	Verify the configuration.

This example shows how to configure an interface with a backup interface and to verify the configuration:

```
Switch# configure terminal
Switch(conf)# boot host dhcp
Switch(conf)# boot host retry timeout 420
Switch(conf)# banner config-save ^C Caution - Downloading running configuration file
^C
Switch(conf)#
Switch(conf)# show boot
```

Updates to the Command References

These command were added to the *Catalyst 2940 Switch Command Reference, Cisco IOS Release 12.1(22)EA7*:

- boot host, page 40
- banner config-save, page 41
- show boot, page 42

boot host

To specify the mechanism used to download a configuration file at the next system startup, use the **boot host** global configuration command. To restore the host configuration filename to the default, use the **no** form of this command.

boot host {**dhcp** | **retry** *timeout*}

no boot host {**dhcp** | **retry** *timeout*}

Syntax Description

dhcp	Specify the system to get an IP address, configuration file, and TFTP server address using DHCP.
retry *timeout*	Specify the amount of time between retries; valid values are between 60 and 65,535 seconds.

Defaults

The timeout is zero.

Command Modes

Global configuration

Command History

Release	Modification
12.1(22)EA7	This command was introduced.

Usage Guidelines

If you configure boot host dhcp it will only take effect in the next reboot.

If you enter the **no boot host dhcp** command while the boot host dhcp is waiting for the retry timer to expire the system will stops trying, however if the configuration download is in progress, the system continues to download.

Examples

The following example enables the download of a configuration file at the next system startup:

```
Switch(config)# boot host dhcp
```

The following example sets the time before retries to 420 seconds:

```
Switch(config)# boot host retry timeout 420
```

Related Commands

Command	Description
banner config-save	Displays a configuration banner.

banner config-save

To display a configuration banner, use the **banner config-save** global configuration command. The no form of this command deletes the configuration banner.

banner config-save ^c *message* **^c**

no banner config-save

Syntax Description

^c	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	Message text. You can include tokens in the form $(token) in the message text. Tokens are replaced with the corresponding configuration variable and are described in Table 11.

Defaults

No banner is displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.1(22)EA7	This command was introduced.

Usage Guidelines

To customize the banner, use tokens in the form $(token) in the message text. Tokens display current IOS configuration variables, such as the switchs hostname and IP address. The tokens are described in Table 10.

Table 10 banner login command tokens

Token	Information displayed in the banner
$(hostname)	Displays the switchs hostname.
$(domain)	Displays the switchs domain name.
$(line)	Displays the VTY or TTY (async) line number.
$(line-desc)	Displays the description attached to the line.

Examples

The following example sets a config-save banner:

```
Switch(config)# banner config-save ^c
Caution-Downloading Running Configuration File
^C
```

show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

show boot [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(22)EA7	Updated output to display Timeout for Config Download and Config Download via DHCP.

Usage Guidelines

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

Note Only the software can read and write a copy of the private configuration file. You cannot read, write, delete, or display a copy of this file.

Examples

This is an example of output from the **show boot** command. Table 11 describes each field in the output.

```
Switch# show boot
BOOT path-list:
Config file:         flash:config.text
Private Config file: flash:private-config.text
Enable Break:        no
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
buffer size:   32768
Timeout for Config
     Download: 200 seconds
Config Download
     via DHCP: enabled (next boot: enabled)
```

Table 11 show boot Field Descriptions

Field	Description
BOOT path-list	Displays a semicolon-separated list of executable files to load and to execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
Config file	Displays the filename that the software uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that the software uses to read and write a nonvolatile copy of the private configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to *yes*, *on*, or *1*, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to *no* or *0*, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
NVRAM/Config file buffer size	Displays the buffer size that the software uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation.

Table 11 show boot Field Descriptions (continued)

Field	Description
Timeout for Config Download	Displays the the retry timeout, the time boot host DHCP tries to download the configuration.
Config Download via DHCP	Displays if boot host DHCP feature is enabled for this boot and the subsequent boot.

Related Commands

Command	Description
boot private-config-file	Specifies the filename that the software uses to read and write a nonvolatile copy of the private configuration.
boot host	Specifies the switch to download a configuration file at the next system startup.

Documentation Updates in Cisco IOS Release 12.1(22)EA6

These are the updates to the product documentation that occurred in Cisco IOS Release 12.1(22)EA6:

Updates for the Software Configuration Guides

On Catalyst 2955 and 2950 switches, you can enable IEEE 802.1x on an RSPAN destination or an RSPAN reflector port but not on a SPAN destination port.

These are the updates for the "Using IEEE 802.1x with Guest VLAN" section in the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the software configuration guides for this release:

You can enable optional guest VLAN behavior by using the **dot1x guest-vlan supplicant** global configuration command. When enabled, the switch does not maintain the EAPOL packet history and allows clients that fail authentication to access the guest VLAN, regardless of whether EAPOL packets had been detected on the interface. Clients that fail authentication can access the guest VLAN.

Note Depending on the switch configuration, this process can take up to several minutes.

Updates for the Command References

On the Catalyst 2955 and 2950 switches, the **loopback** keyword in the **errdisable detect cause** global configuration command was added in Cisco IOS Release 12.1(13)EA1.

Updates for the System Message Guides

This system message was added:

Error Message `DOT1X-5-ERR_SPANDST: Dot1x can not be enabled on [chars]. It is configured as a SPAN Dest port.`

Explanation This message means that IEEE 802.1x and SPAN destination ports are mutually exclusive features. [chars] is a port.

Recommended Action Disable the SPAN destination port configuration before reconfiguring IEEE 802.1x on the port.

Updates to the Regulatory Compliance and Safety Information and the Hardware Installation Guides

This information was added to the *Regulatory Compliance and Safety Information* for the Catalyst 2950 and 2940 switches and to the *Catalyst 2955 Switch Hardware Installation Guide*:

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.**

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.**

Figyelem **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 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。

Documentation Updates in Cisco IOS Release 12.1(22)EA5

These are the updates to the product documentation that occurred in Cisco IOS Release 12.1(22)EA5:

- "Updates for the Software Configuration Guides" section on page 47
- "Updates for the Hardware Installation Guides" section on page 47

Updates for the Software Configuration Guides

These are the updates for the "Using IEEE 802.1x with Guest VLAN" section in the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the software configuration guides for this release:

With Cisco IOS Release 12.1(22)EA5 and later, the switch maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to the interface is an IEEE 802.1x-capable supplicant, and the interface does not change to the guest VLAN state. The EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, it changes to the guest VLAN state.

Note If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface changes to an unauthorized state, and 802.1x authentication restarts.

These are updates for the "Configuring IEEE 802.3z Flow Control on Gigabit Ethernet Ports" section in the "Configuring Interface Characteristics" chapter of the software configuration guides for this release:

The section should be called "Configuring IEEE 802.3x Flow Control on IEEE 802.3z Gigabit Ethernet Ports," and references to IEEE 802.3z flow control should be IEEE 802.3x flow control.

Updates for the Hardware Installation Guides

These are the updates for the "Installing the Switch" section in the "Installation" chapter of the Hardware Installation guide for the Catalyst 2940:

Catalyst 2940 Rack-Mounting

This installation procedure covers 19-inch rack-mounting.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

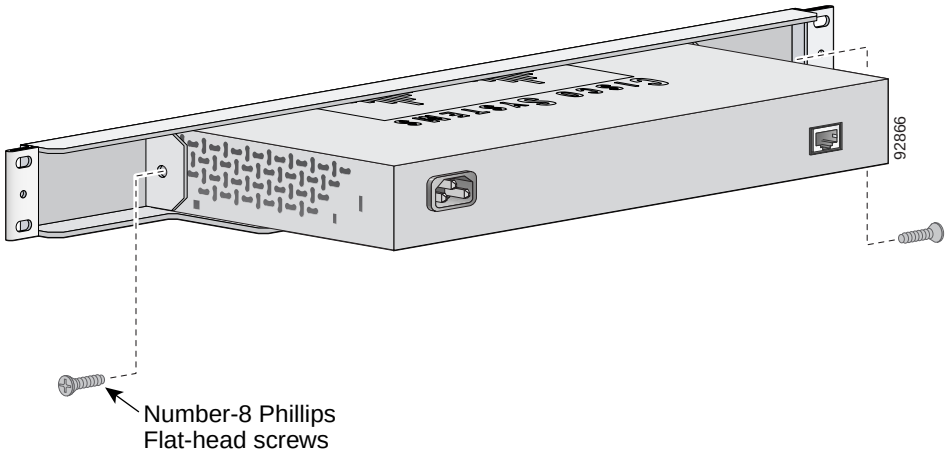
This unit should be mounted at the bottom of the rack if it is the only unit in the rack.

When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

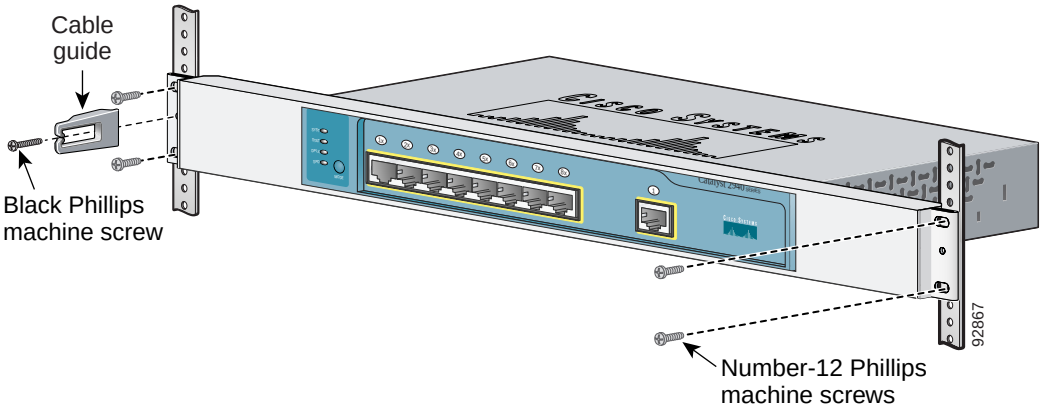
If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
Statement 1006

Follow these steps:

Step 1 Position the switch in the center of the mounting bracket.



Step 2 Insert a number-8 Phillips flat-head screw through the bracket into one side of the switch. Tighten the screw with a screwdriver. Repeat on the opposite side.



Step 3 Align the switch bracket assembly in the rack. Insert the number-12 Phillips machine screws through the bracket into the rack. Tighten the screws with a screwdriver. Repeat on the opposite side.

Step 4 Use the black Phillips machine screw to attach the cable guide to either bracket.

Translated Safety Warning

This section includes translations in multiple languages of the warnings that might appear in your product documents.

Statement 1006—Chassis Warning for Rack-Mounting and Servicing

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.**

Waarschuwing **Om lichamelijk letsel te voorkomen wanneer u dit toestel in een rek monteert of het daar een servicebeurt geeft, moet u speciale voorzorgsmaatregelen nemen om ervoor te zorgen dat het toestel stabiel blijft. De onderstaande richtlijnen worden verstrekt om uw veiligheid te verzekeren:**

- **Dit toestel dient onderaan in het rek gemonteerd te worden als het toestel het enige in het rek is.**
- **Wanneer u dit toestel in een gedeeltelijk gevuld rek monteert, dient u het rek van onderen naar boven te laden met het zwaarste onderdeel onderaan in het rek.**
- **Als het rek voorzien is van stabiliseringshulpmiddelen, dient u de stabilisatoren te monteren voordat u het toestel in het rek monteert of het daar een servicebeurt geeft.**

Varoitus **Kun laite asetetaan telineeseen tai huolletaan sen ollessa telineessä, on noudatettava erityisiä varotoimia järjestelmän vakavuuden säilyttämiseksi, jotta vältytään loukkaantumiselta. Noudata seuraavia turvallisuusohjeita:**

- **Jos telineessä ei ole muita laitteita, aseta laite telineen alaosaan.**
- **Jos laite asetetaan osaksi täytettyyn telineeseen, aloita kuormittaminen sen alaosasta kaikkein raskaimmalla esineellä ja siirry sitten sen yläosaan.**
- **Jos telinettä varten on vakaimet, asenna ne ennen laitteen asettamista telineeseen tai sen huoltamista siinä.**

Attention **Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel :**

- **Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.**
- **Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.**
- **Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.**

Warnung **Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:**

- **Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.**
- **Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.**
- **Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.**

Avvertenza **Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un supporto, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive vengono fornite per garantire la sicurezza personale:**

- **Questa unità deve venire montata sul fondo del supporto, se si tratta dell'unica unità da montare nel supporto.**
- **Quando questa unità viene montata in un supporto parzialmente pieno, caricare il supporto dal basso all'alto, con il componente più pesante sistemato sul fondo del supporto.**
- **Se il supporto è dotato di dispositivi stabilizzanti, installare tali dispositivi prima di montare o di procedere alla manutenzione dell'unità nel supporto.**

Advarsel **Unngå fysiske skader under montering eller reparasjonsarbeid på denne enheten når den befinner seg i et kabinett. Vær nøye med at systemet er stabilt. Følgende retningslinjer er gitt for å verne om sikkerheten:**

- **Denne enheten bør monteres nederst i kabinettet hvis dette er den eneste enheten i kabinettet.**
- **Ved montering av denne enheten i et kabinett som er delvis fylt, skal kabinettet lastes fra bunnen og opp med den tyngste komponenten nederst i kabinettet.**
- **Hvis kabinettet er utstyrt med stabiliseringsutstyr, skal stabilisatorene installeres før montering eller utføring av reparasjonsarbeid på enheten i kabinettet.**

Aviso **Para se prevenir contra danos corporais ao montar ou reparar esta unidade numa estante, deverá tomar precauções especiais para se certificar de que o sistema possui um suporte estável. As seguintes directrizes ajudá-lo-ão a efectuar o seu trabalho com segurança:**

- **Esta unidade deverá ser montada na parte inferior da estante, caso seja esta a única unidade a ser montada.**
- **Ao montar esta unidade numa estante parcialmente ocupada, coloque os itens mais pesados na parte inferior da estante, arrumando-os de baixo para cima.**
- **Se a estante possuir um dispositivo de estabilização, instale-o antes de montar ou reparar a unidade.**

¡Advertencia! **Para evitar lesiones durante el montaje de este equipo sobre un bastidor, o posteriormente durante su mantenimiento, se debe poner mucho cuidado en que el sistema quede bien estable. Para garantizar su seguridad, proceda según las siguientes instrucciones:**

- **Colocar el equipo en la parte inferior del bastidor, cuando sea la única unidad en el mismo.**
- **Cuando este equipo se vaya a instalar en un bastidor parcialmente ocupado, comenzar la instalación desde la parte inferior hacia la superior colocando el equipo más pesado en la parte inferior.**
- **Si el bastidor dispone de dispositivos estabilizadores, instalar éstos antes de montar o proceder al mantenimiento del equipo instalado en el bastidor.**

Varning! **För att undvika kroppsskada när du installerar eller utför underhållsarbete på denna enhet på en ställning måste du vidta särskilda försiktighetsåtgärder för att försäkra dig om att systemet står stadigt. Följande riktlinjer ges för att trygga din säkerhet:**

- **Om denna enhet är den enda enheten på ställningen skall den installeras längst ned på ställningen.**
- **Om denna enhet installeras på en delvis fylld ställning skall ställningen fyllas nedifrån och upp, med de tyngsta enheterna längst ned på ställningen.**
- **Om ställningen är försedd med stabiliseringsdon skall dessa monteras fast innan enheten installeras eller underhålls på ställningen.**

Figyelem **A készülék rackbe történő beszerelése és karbantartása során bekövetkező sérülések elkerülése végett speciális óvintézkedésekkel meg kell őrizni a rendszer stabilitását. A személyes biztonsága érdekében tartsa be a következő szabályokat:**

- **Ha a rackben csak ez az egy készülék található, a rack aljába kell beszerelni.**
- **Ha nincs teljesen tele az a rack, amelybe beszerelik a készüléket, alulról fölfelé haladva töltse fel a racket úgy, hogy a legnehezebb készülék kerüljön a rack aljába.**
- **Ha stabilizáló eszközök is tartoznak a rackhez, szerelje fel a stabilizátorokat, mielőtt beszerelné az egységet a rackbe, vagy karbantartást végezne rajta.**

Предупреждение Во избежание травм при монтаже и обслуживании устройства в стойке следует принять особые меры предосторожности, чтобы убедиться в устойчивости оборудования.
Для обеспечения безопасности работ необходимо соблюдать следующие правила.

- Если в стойке находится одно устройство, оно должно быть установлено в нижней части.
- При монтаже устройств в частично заполненную стойку устанавливайте оборудование снизу вверх, размещая наиболее тяжелые устройства в нижней части.
- Если стойка снабжена приспособлениями для стабилизации, их необходимо установить до начала монтажа или обслуживания оборудования.

警告 为避免在机架中安装或维修该部件时使身体受伤，您必须采取特殊的预防措施确保系统固定。以下是确保安全的原则：

- 如果此部件是机架中唯一的部件，应将其安装在机架的底部。
- 如果在部分装满的机架中安装此部件，请按从下往上的顺序安装各个部件，并且最重的组件应安装在机架的底部。
- 如果机架配有固定装置，请先装好固定装置，然后再在机架中安装或维修部件。

警告 この装置をラックに設置したり保守作業を行ったりするときは、人身事故を防ぐため、システムが安定しているかどうかを十分に確認する必要があります。次の注意事項に従ってください。

- ラックにこの装置を単独で設置する場合は、ラックの一番下に設置します。
- ラックに別の装置がすでに設置されている場合は、最も重量のある装置を一番下にして、重い順に下から上へ設置します。
- ラックに安定器具が付属している場合は、その安定器具を取り付けてから、装置をラックに設置するか、またはラック内の装置の保守作業を行ってください。

주의 이 장치를 랙에 장착하거나 서비스할 때 신체 부상을 방지하려면, 시스템이 안정된 상태를 유지하도록 특별히 주의해야 합니다. 사용자의 안전을 위해 다음 지침 사항을 준수하십시오.

- 이 장치가 랙에 장착되는 유일한 것일 경우, 랙의 맨 아래 부분에 장착되어야 합니다.
- 부분적으로 차 있는 랙에 이 장치를 장착할 경우, 가장 무거운 장치를 랙의 맨 아래 부분부터 차례로 장착하십시오.
- 안정기가 랙과 함께 제공되는 경우, 이 안정기를 설치한 후 이 장치를 랙에 장착하거나 서비스하십시오

Aviso **Para evitar lesões corporais ao montar ou dar manutenção a esta unidade em um rack, é necessário tomar todas as precauções para garantir a estabilidade do sistema. As seguintes orientações são fornecidas para garantir a sua segurança:**

- **Se esta for a única unidade, ela deverá ser montada na parte inferior do rack.**
- **Ao montar esta unidade em um rack parcialmente preenchido, carregue-o de baixo para cima com o componente mais pesado em sua parte inferior.**
- **Se o rack contiver dispositivos estabilizadores, instale-os antes de montar ou dar manutenção à unidade existente.**

Advarsel **For at forhindre legemesbeskadigelse ved montering eller service af denne enhed i et rack, skal du sikre at systemet står stabilt. Følgende retningslinjer er også for din sikkerheds skyld:**

- **Enheden skal monteres i bunden af dit rack, hvis det er den eneste enhed i racket.**
- **Ved montering af denne enhed i et delvist fyldt rack, skal enhederne installeres fra bunden og opad med den tungeste enhed nederst.**
- **Hvis racket leveres med stabiliseringsenheder, skal disse installeres for enheden monteres eller serviceres i racket.**

تحذير **لتجنب حدوث أي إصابات عند تركيب هذه الوحدة، يجب اتباع بعض الاحتياطات لضمان عمل النظام بشكل سليم.**
يتم ذكر الإرشادات التالية لضمان الأمان.
يجب تركيب هذه الوحدة في الجزء السفلي من الدولاب المتضمن قضبان إذا كانت هذه الوحدة هي الوحدة الوحيدة في الدولاب الذي يحتوي على قضبان.
عند تركيب هذه الوحدة في دولاب شبه ممتلئ، قم برفع الدولاب من الجزء السفلي لأعلى بحيث يكون الجزء الأثقل وزناً أسفل الدولاب.
إذا كان الدولاب المتضمن قضباناً يحتوي على أجهزة حفظ التوازن، قم بتثبيت هذه الأجهزة قبل تركيب الوحدة في الدولاب.

Upozorenje **Kako ne bi došlo do tjelesnih ozljeda kod postavljanja ili servisiranja uređaja na polici, potrebno je poduzeti mjere predostrožnosti kako bi sustav uvijek bio stabilan. Sigurnost se može osigurati poštivanjem sljedećih smjernica:**
- **Ovaj uređaj treba ugraditi na dno police, ukoliko je to jedini uređaj na polici.**
- **Kod ugradnje uređaja u policu na kojoj se već nalaze drugi uređaji, policu treba opremati počevši od dna, te tako da se na dno stave najteži dijelovi.**
- **Ukoliko su na polici ugrađeni stabilizatori, njih montirajte prije ugradnje ili servisiranja uređaja na polici.**

Upozornění **Abyste předešli poranění osob při montáži nebo opravě zařízení v montážním rámu, musíte dodržovat zvláštní preventivní opatření pro zajištění udržení stability systému. Pro zajištění bezpečnosti obsluhy jsou určeny následující zásady:**
- **Pokud je toto zařízení jedinou jednotkou v montážním rámu, musí být namontováno na nejnižší místo rámu.**
- **Pokud je toto zařízení montováno do částečně obsazeného montážního rámu, obsazujte montážní rám ve směru zdola nahoru tak, aby byla nejtěžší součást nejníže.**
- **Pokud je montážní rám vybaven stabilizačními zařízeními, nainstalujte stabilizátory ještě před montáží nebo opravou zařízení v montážním rámu.**

Για να αποφύγετε τον τραυματισμό κατά την τοποθέτηση ή τη συντήρηση αυτής της συσκευής σε αρθρωτό σύστημα, πρέπει να λάβετε ειδικές προφυλάξεις για να διασφαλίσετε τη σταθερότητα του συστήματος. Οι παρακάτω οδηγίες παρέχονται για να εξασφαλίσουν την ασφάλειά σας:

- Αυτή η συσκευή πρέπει να τοποθετείται στο κάτω μέρος του αρθρωτού συστήματος αν είναι η μοναδική συσκευή σε αυτό.
- Όταν τοποθετείτε αυτήν τη συσκευή σε εν μέρει γεμάτο αρθρωτό σύστημα, τοποθετήστε συσκευές στο αρθρωτό σύστημα από κάτω προς τα επάνω, με τη βαρύτερη συσκευή στο κάτω μέρος του συστήματος.
- Εάν το αρθρωτό σύστημα διαθέτει διατάξεις σταθεροποίησης, τοποθετήστε τους σταθεροποιητές πριν τοποθετήσετε ή συντηρήσετε τη συσκευή στο αρθρωτό σύστημα.

אזהרה

כדי למנוע פציעה בעת הרכבת יחידה זו במעמד או טיפול בה, עליך לנקוט אמצעי זהירות מיוחדים כדי להבטיח את יציבות המערכת. הקווים המנחים הבאים ניתנים על מנת להבטיח את ביטחונך:

- אם יחידה זו היא יחידה בודדת במעמד, יש להרכיב את היחידה בחלקו התחתון של המעמד.
- בעת הרכבת יחידה זו במעמד המלא בחלקו, טען את המעמד החל בחלק התחתון וכלפי מעלה כאשר הרכיב הכבד ביותר נמצא בחלקו התחתון של המעמד.
- אם המעמד מסופק עם התקני ייצוב, התקן את המייצבים לפני הרכבה היחידה במעמד או טיפול בה.

Opomena

За да се не повредите кога го монтирате или го сервисирате уредот на полица, мора да бидете особено претпазливи за да ја обезбедите стабилноста на системот. Следите напатствија се дадени за да ја осигураат Вашата безбедност:

- Уредот треба да се монтира најдолу на полицата ако е единствен уред на полицата.
- Кога го монтирате уредот на делумно пополнета полица, полнете ја полицата од дното кон врвот со најтешката компонента на дното на полицата.
- Ако полицата има стабилизаторски делови, наместете ги стабилизаторите пред да го монтирате или сервисирате уредот на полицата.

Ostrzeżenie **Aby zapobiec urazom podczas montażu lub serwisowania tego urządzenia w stojaku, należy zastosować szczególne środki ostrożności w celu zapewnienia stabilności układu. Poniżej przedstawiono wskazówki, których przestrzeganie zapewni bezpieczeństwo:**
- **Jeśli urządzenie to jest jedynym urządzeniem w stojaku, powinno być zamontowane na dole.**
- **W przypadku montażu urządzenia w częściowo zapełnionym stojaku należy instalować kolejne urządzenia od najniższego do najwyższego, przy czym element najcięższy powinien być zamontowany najniżej w stojaku.**
- **Jeśli stojak jest wyposażony w elementy stabilizujące, należy zamontować stabilizatory przed przystąpieniem do montażu lub serwisowania urządzeń w stojaku.**

Upozornenie **Aby ste predišli poraneniu osôb pri montáži alebo oprave zariadenia v montážnom ráme, musíte dodržiavať zvláštne preventívne opatrenia na zaistenie udržania stability systému. Na zaistenie bezpečnosti obsluhy sú určené nasledujúce zásady:**
- **Pokiaľ je toto zariadenie jedinou jednotkou v montážnom ráme, musí byť namontované na najnižšie miesto v ráme.**
- **Pokiaľ je toto zariadenie montované do čiastočne obsadeného montážneho rámu, obsadzujte montážny rám v smere zdola nahor tak, aby bola najťažšia súčasť najnižšie.**
- **Pokiaľ je montážny rám vybavený stabilizačnými zariadeniami, nainštalujte stabilizátory ešte pred montážou alebo opravou zariadenia v montážnom ráme.**

Related Documentation

These documents provide complete information about the Catalyst 2955, 2950, and 2940 switches and are available at Cisco.com:

http://www.cisco.com/en/US/products/ps6738/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/hw/switches/ps628/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/hw/switches/ps4916/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/hw/switches/ps5213/tsd_products_support_series_home.html

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 55.

- *Catalyst 2955, 2950, and 2940 Switch System Message Guide* (not orderable but available on Cisco.com)

These publications provide more information about the Catalyst 2955 and Catalyst 2950 switches:

- *Catalyst 2950 and Catalyst 2955 Desktop Switch Software Configuration Guide* (order number DOC-7811380=)
- *Catalyst 2950 and Catalyst 2955 Desktop Switch Command Reference* (order number DOC-7811381=)
- Device manager online help (available on the switch)

- *Catalyst 2950 Desktop Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2950 Switch Getting Started Guide (*order number DOC-1786521=)
- *Regulatory Compliance and Safety Information for the Catalyst 2950 Switch* (order number DOC-7816625=)
- *Catalyst 2955 Hardware Installation Guide* (order number DOC-7814944=)

These publications provide more information about the Catalyst 2940 switches:

- *Catalyst 2940 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 2940 Switch Command Reference* (not orderable but available on Cisco.com))
- Device manager online help (available on the switch)
- *Catalyst 2940 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2940 Switch Getting Started Guide (*order number DOC-7816576=)
- *Regulatory Compliance and Safety Information for the Catalyst 2940 Switch* (order number DOC-7816656=)

For other information about related products, see these documents:

- *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)
- *1000BASE-T Gigabit Interface Converter Installation Notes* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)
- *Cisco LRE CPE Hardware Installation Guide* (order number DOC-7811469=)
- *CWDM Passive Optical System Installation Note* (not orderable but is available on Cisco.com)
- *Installation Notes for the Catalyst Family Small-Form-Factor Pluggable Modules* (order number DOC-7815160=)
- *Installation and Warranty Notes for the Cisco LRE 48 POTS Splitter* (order number DOC-7812250=)
- *Network Admission Control Software Configuration Guide* (not orderable but is available on Cisco.com

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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