



# Release Notes for the Catalyst 2955, Catalyst 2950, and Catalyst 2940 Switches, Cisco IOS Release 12.1(22)EA4 and Later

---

**Revised November 2, 2005**

Cisco IOS Release 12.1(22)EA4 and later run 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 Cisco IOS release 12.1(22)EA4, and 12.1(22)EA4a 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 30.

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)EA4 is based on Cisco IOS Release 12.1(22)E5. Open caveats in Cisco IOS Release 12.1(22)E5 also affect Cisco IOS Release 12.1(22)EA4 unless they are listed in the Cisco IOS Release 12.1(22)EA4 resolved caveats list. The list of open caveats in Cisco IOS Release 12.1(22)E5 is available at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12\\_1e/ol\\_2310.htm#wp1560107](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/ol_2310.htm#wp1560107)



---

**Corporate Headquarters:**

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

# Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Upgrading the Switch Software” section on page 6](#)
- [“Installation Notes” section on page 13](#)
- [“New Features” section on page 13](#)
- [“Limitations and Restrictions” section on page 14](#)
- [“Important Notes” section on page 24](#)
- [“Open Caveats” section on page 27](#)
- [“Resolved Caveats” section on page 27](#)
- [“Documentation Updates” section on page 29](#)
- [“Related Documentation” section on page 30](#)
- [“Obtaining Documentation” section on page 31](#)
- [“Cisco Product Security Overview” section on page 32](#)
- [“Obtaining Technical Assistance” section on page 33](#)
- [“Obtaining Additional Publications and Information” section on page 34](#)

## System Requirements

The system requirements for this release are described in these sections:

- [“Hardware Supported” section on page 2](#)
- [“Hardware Not Supported” section on page 4](#)
- [“Device Manager System Requirements” section on page 4](#)
- [“Cluster Compatibility” section on page 5](#)

## 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 22](#).

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	— <sup>1</sup>	8 10/100 Ethernet ports and 1 10/100/1000 Ethernet port
Catalyst 2940-8TF-S	— <sup>1</sup>	8 10/100 Ethernet ports, 1 SFP <sup>2</sup> 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 <sup>3</sup> 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 <sup>4</sup> , and 2 SFP module slots
Catalyst 2950ST-24 LRE	EI	24 LRE ports, 2 10/100/1000 Ethernet ports <sup>4</sup> , and 2 SFP module slots
Catalyst 2950ST-24 LRE 997	EI	24 LRE ports, 2 10/100/1000 Ethernet ports <sup>4</sup> , 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 autosensing 10/100 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 <sup>5</sup>
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 <sup>6</sup> 100BASE-FX ports
Catalyst 2955S-12	EI	12 fixed autosensing 10/100 ports and 2 SM <sup>7</sup> 100BASE-LX ports
Catalyst 2955T-12	EI	12 fixed autosensing 10/100 ports and 2 10/100/1000 Ethernet ports <sup>4</sup>

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 <sup>1</sup>	—	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	—	<ul style="list-style-type: none"> <li>• 1000BASE-SX GBIC</li> <li>• 1000BASE-LX/LH GBIC</li> <li>• 1000BASE-ZX GBIC</li> <li>• 1000BASE-T GBIC (model WS-5483)</li> <li>• CWDM<sup>2</sup> fiber-optic GBIC<sup>3</sup></li> <li>• DWDM<sup>4</sup> fiber-optic GBIC</li> <li>• GigaStack GBIC</li> </ul>
Redundant power system	—	<ul style="list-style-type: none"> <li>• Cisco RPS 300 redundant power system</li> <li>• Cisco RPS 675 redundant power system</li> </ul>
SFP devices	—	<ul style="list-style-type: none"> <li>• 1000BASE-SX SFP module</li> <li>• 1000BASE-LX\LH SFP module</li> <li>• 1000BASE-ZX SFP module</li> <li>• 1000BASE-T SFP module</li> <li>• CWDM</li> </ul>

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 <sup>1</sup>	64 MB <sup>2</sup>	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 <sup>1</sup>	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.

# 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](#)
- [“Upgrading a Switch by Using the Device Manager or Network Assistant” section on page 8](#)
- [“Upgrading a Switch by Using the CLI” section on page 8](#)
- [“Recovering from Software Failure” section on page 13](#)

For information about the software releases that support the switches, see the [“Catalyst 2950 Hardware and Software Compatibility Matrixes” section on page 22](#).

**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.EA4a.tar	Catalyst 2955 EI files. This includes the cryptographic Cisco IOS image and the device manager files.
c2955-i6q4l2-tar.121-22.EA4a.tar	Catalyst 2955 EI files. This includes the Cisco IOS image and the device manager files.
c2950-i6k2l2q4-tar.121-22.EA4a.tar	Catalyst 2950 SI <sup>1</sup> and EI files. This includes the cryptographic Cisco IOS image and the device manager files.
c2950-i6q4l2-tar.121-22.EA4a.tar	Catalyst 2950 SI and EI files. This includes the Cisco IOS image and the device manager files.
c2950lre-i6k2l2q4-tar.121-22.EA4a.tar	Catalyst 2950 LRE EI files. This includes the cryptographic Cisco IOS image and the device manager files.
c2950lre-i6l2q4-tar.121-22.EA4a.tar	Catalyst 2950 LRE EI files. This includes the Cisco IOS image and the device manager files.

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

Filename	Description
c2940-i6k2l2q4-tar.121-22.EA4a.tar	Catalyst 2940 files. This includes the cryptographic Cisco IOS image and the device manager files.
c2940-i6q4l2-tar.121-22.EA4a.tar	Catalyst 2940 files. This includes the Cisco IOS image and the device manager files.

- 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 14](#).

## 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 menu bar, select **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:

- Download the tar files from Cisco.com, as described in the “[Downloading the Software](#)” section on [page 8](#).
- Copy the current startup configuration file, as described in the “[Copying the Current Startup Configuration from the Switch to a PC or Server](#)” section on [page 9](#).
- 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 9](#).
  - 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 11](#).

## 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 a PC or 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.EA4/`
- 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.EA4.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-i6q412-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-i6q412-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.  
See the “Quick Setup” chapter in the Catalyst 2950 and Catalyst 2940 getting started guides for more information about Express Setup.
- 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 13](#)
- [“New Software Features” section on page 14](#)

## New Hardware Features

For a complete list of supported hardware, see the [“Hardware Supported” section on page 2](#).

## New Software Features

This release has these new Catalyst 2940, 2950, and 2955 switch enhancements:

- IEEE 802.1x with VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN (Catalyst 2950 switches running the SI).
- Multicast traffic on an EtherChannel is load-balanced across the links in the channel when you configure load balancing based on destination MAC address by using the **port-channel load-balance dst-mac** global configuration command.

## 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 14](#)
- [“LRE Limitations and Restrictions” section on page 20](#)
- [“Device Manager Limitations and Restriction” section on page 22](#)
- [“Catalyst 2950 Hardware and Software Compatibility Matrixes” section on page 22](#)

## 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.

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 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)

- When you use only Catalyst 2950 switches for RSPAN, you cannot monitor traffic in the receive (Rx) direction. You can only monitor traffic in the transmit (Tx) direction.

There is no workaround. (CSCed19922)

- (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)

- If packets with a bad cyclic redundancy check (CRC) are received on a port, the switch might learn the source MAC address of the bad packet.

There is no workaround. (CSCef15178)

- CSCeg41561

When a PC is attached to a switch through a hub, is authenticated on an IEEE 802.1x multiple-hosts port, is moved to another port, and is then attached through another hub, the switch does not authenticate the PC.

The workaround is to decrease the number of seconds between re-authentication attempts by entering the **dot1x timeout reauth-period** *seconds* interface configuration command.

- 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 <sup>1</sup> port <sup>2</sup> | No            | No                              |
| Trunk port                         | No            | No                              |
| Dynamic-access port <sup>3</sup>   | No            | No                              |
| SPAN source port                   | Yes           | Yes                             |
| SPAN destination port              | No            | No                              |
| EtherChannel                       | No            | No                              |
| Protected port                     | Yes           | Yes                             |
| IEEE 802.1x port                   | —             | Yes <sup>4</sup>                |
| Voice VLAN port <sup>5</sup>       | 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/up. There is no workaround to the issue itself. However you can use aggressive mode UDLD when suitable. (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 13.
- 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*

| <b>Hardware</b>   | <b>Serial Number</b>                        | <b>Cisco IOS Release 12.0(5)WC2b or Earlier</b> | <b>Cisco IOS Release 12.1(6)EA2, 12.1(6)EA2a, and 12.1(6)EA2b</b> | <b>Cisco IOS Release 12.1(6)EA2c</b> | <b>Cisco IOS Release 12.1(9)EA1 or Later</b> |
|-------------------|---------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------|--------------------------------------|----------------------------------------------|
| 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 24](#)
- [“Device Manager Notes” section on page 25](#)

## 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.

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

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

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

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

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

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

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

## Open Caveats

This section describes the open caveats with possible unexpected activity in this software release.

- CSCdx95501

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
```

- CSCeg49056 (Catalyst 2950 LRE switches)

The switch reloads when this message appears:

```
Signal 5, Exception code (0x0024)!, PC 0x80565714
```

There is no workaround.

- CSCeh16869

In an multiple spanning-tree (MST) region in which Switch 1 is connected to Switch 2 and Switch 2 is connected to Switch 3, if Switch 2 has a root port and a designated port in MST instance 2, the root port flaps. The designated port is not synchronized with the other switches in the MST region, and the convergence of the port from the blocking state to the learning state is slow.

The workaround is to modify the switch priority to a lower value so that the Switch 2 becomes the root switch for the MST instances 0 and 2.

## Resolved Caveats

These sections describe the caveats have been resolved in this release. All resolved caveats listed in these sections apply to the Catalyst 2955, Catalyst 2950, and Catalyst 2940 switches unless otherwise noted.

- [Resolved IOS Caveats in Cisco IOS Release 12.1\(22\)EA4a](#)
- [Resolved IOS Caveats in Cisco IOS Release 12.1\(22\)EA4](#)

## Resolved IOS Caveats in Cisco IOS Release 12.1(22)EA4a

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCei76358  
Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

## Resolved IOS Caveats in Cisco IOS Release 12.1(22)EA4

- CSCeb84447 (Catalyst 2940 switches)  
If an SFP module interface is disabled, the interface on the connected device no longer remains enabled.
- CSCef60659  
A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).  
These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:
  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages
 Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.  
Multiple Cisco products are affected by the attacks described in this Internet draft.  
Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.  
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.  
The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.
- CSCeg15130  
If multiple switches are configured in a multicast television application in which Multicast VLAN Registration (MVR) is enabled and MVR ports are statically configured, IGMP leave messages are no longer sent to the router.  
In previous releases, IGMP leave messages were sent to the router under these conditions. IGMP leave messages should not have been sent with statically-configured MVR ports registered for the multicast stream.
- CSCeg47968  
On rare occasions, 100BASE-FX interfaces on switches running Cisco IOS Release 12.1(22)EA3 and earlier might send packets but not receive packets, creating a spanning-tree loop. This problem no longer occurs in switches running Cisco IOS Release 12.1(22)EA4 and later.

- CSCeg53741  
If frame sizes larger than 1518 bytes are received and the system MTU is configured as 1530 bytes, the counters no longer display the packets as *giants*.
- CSCeg57925  
The switch no longer stops if a port that is assigned to the management VLAN does not have a corresponding access VLAN.
- CSCeg58877 (Catalyst 2950 switches)
- If a switch uses rapid per-VLAN spanning tree plus (rapid-PVST+), a loop no longer occurs when you reconfigure the allowed VLANs on a trunk and remove the native VLAN from the trunk.
- CSCeg64254 (Catalyst 2940 switches)  
When a 10/100/1000 port (in Catalyst 2940 switches running Cisco IOS Release 12.1(22)EA2) is set to 100 Mbps and full-duplex mode, the switch no longer comes up in 100 Mbps and half-duplex mode when the switch is reloaded.
- CSCeg68041  
Multicast traffic on an EtherChannel now load-balances across the links in the channel when you configure load balancing based on destination MAC address by using the **port-channel load-balance dst-mac** global configuration command.
- CSCeg77063  
If there are no active ports, the MAC address-table aging-time configuration now appears in the **show running-config** privileged EXEC command output.
- CSCeg77968  
When an IEEE 802.1x is enabled on a port, there is no longer a 10-second delay before the switch sends an EAP-request/identity frame.
- CSCeh05090 (Catalyst 2955 and Catalyst 2950 switches)  
During an RSPAN session, multicast traffic now reaches the RSPAN destination port.
- CSCeh38060  
A switch stack no longer generates unnecessary topology change notifications (TCNs) under these conditions:
  - The stack contains three or more switches. Catalyst 3750 switches can be stacked by using the Stackwise connection. Other Catalyst switches can be stacked by using a Gigastack GBIC.
  - The stack is running either Cisco IOS Release 12.2(25)SEA or Cisco IOS Release 12.1(22)EA3. (This caveat does not affect any other Cisco IOS release.)
  - The stack is running cross-stack rapid transition (CSRT) and rapid PVST.

## Documentation Updates

For the documentation updates, see the *Documentation Updates for the Catalyst 2955, Catalyst 2950, and Catalyst 2940 Switches, Cisco IOS Release 12.1(22)EA4* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12122ea4/index.htm>

## 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/univercd/cc/td/doc/product/lan/cat2950/index.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2940/index.htm>

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 31.

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=)
- *Catalyst 2950 and Catalyst 2955 Desktop Switch System Message Guide* (order number DOC-7814233=)
- 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* (order number DOC-7815507=)
- *Catalyst 2940 Switch Command Reference* (order number DOC-7815505=)
- *Catalyst 2940 Switch System Message Guide* (order number DOC-7815524=)
- 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=)

## 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/univercd/home/home.htm>

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](http://www.cisco.com/public/countries_languages.shtml)

### Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpc/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpc/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)



We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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>

- *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>

- 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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

