



# Release Notes for the Catalyst 2950 Switch Cisco IOS Release 12.1(14)AZ

---

**October 2003**

Cisco IOS Release 12.1(14)AZ runs on Catalyst 2950 switches.



**Note**

---

This release supports only the non-LRE Catalyst 2950 switches.

---

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. To verify that these are the correct release notes for your switch:

- If you are installing a new switch, refer to 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 “[Determining the Software Version and Feature Set](#)” section on page 8.
- If you are upgrading to a new release, refer to the software upgrade filename for the Cisco IOS version.

For the complete list of Catalyst 2950 switch documentation, see the “[Related Documentation](#)” section on page 34.

You can download the switch software from these sites:

- <http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>  
(for registered Cisco.com users with a login password)
- <http://www.cisco.com/public/sw-center/sw-lan.shtml>  
(for nonregistered Cisco.com users)

This 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 releases become available, they will be posted to Cisco.com (previously Cisco Connection Online [CCO]) in the Cisco IOS software area.



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

# Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Downloading Software” section on page 7](#)
- [“Installation Notes” section on page 13](#)
- [“New Features” section on page 16](#)
- [“Limitations and Restrictions” section on page 16](#)
- [“Important Notes” section on page 25](#)
- [“Open Caveats” section on page 27](#)
- [“Documentation Updates” section on page 32](#)
- [“Related Documentation” section on page 34](#)
- [“Ordering Documentation” section on page 35](#)
- [“Obtaining Technical Assistance” section on page 35](#)

## 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](#)
- [“Software Compatibility” section on page 4](#)
- [“Cluster Capability” section on page 6](#)

## Hardware Supported

The Catalyst 2950 switch is supported by either the standard software image (SI) or the enhanced software image (EI).

The EI provides a richer set of features, including access control lists (ACLs), enhanced quality of service (QoS) features, extended-range VLANs, the IEEE 802.1W Rapid Spanning Tree Protocol (RSTP), and the IEEE 802.1S Multiple STP (MSTP). The enhanced crypto software image supports the Secure Shell (SSH) protocol.

For information about the software releases that support the switches listed in [Table 1](#), see the [“Hardware and Software Compatibility Matrixes” section on page 23](#).

Table 1 lists the hardware supported by this release:

**Table 1 Hardware Supported**

Hardware	Software Image	Description
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>1</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 2950SX-24	SI	24 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>2</sup>
Catalyst 2950SX-48-SI	SI	48 fixed autosensing 10/100 Ethernet ports and 2 1000BASE-SX ports.
Catalyst 2950T-48-SI	SI	48 fixed autosensing 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports.
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>3</sup> fiber-optic GBIC<sup>4</sup></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 modules	—	<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> </ul>

1. GBIC = Gigabit Interface Converter
2. The 10/100/1000 interfaces on the Catalyst 2950T-24 switch do not support the **half** keyword in the duplex command.
3. CDWM = Coarse Wave Division Multiplexer
4. This feature is only supported when your switch is running the EI.

## Hardware Not Supported

Table 2 lists the hardware that is not supported by this release:

**Table 2** *Hardware Not Supported*

Hardware	Description
GBIC module	1000BASE-T GBIC (model WS-G5482)
Redundant power system	Cisco RPS 600 Redundant Power System

## Software Compatibility

These are the software compatibility requirements for this release:

- “Recommended Platform Configuration for Web-Based Management” section on page 4
- “Operating System and Browser Support” section on page 4
- “Supported Java Plug-Ins” section on page 5
- “Java Plug-In Notes” section on page 6

## Recommended Platform Configuration for Web-Based Management

Table 3 lists the recommended platforms for web-based management.

**Table 3** *Recommended Platform Configuration for Web-Based Management*

OS	Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Windows NT 4.0 <sup>1</sup>	Pentium 300 MHz	128 MB	65,536	1024 x 768	Small
Solaris 2.5.1 or higher	SPARC 333 MHz	128 MB	Most colors for applications	—	Small (3)

1. Service Pack 3 or higher is required.

The minimum PC requirement is a Pentium processor running at 233 MHz with 64 MB of DRAM. The minimum UNIX workstation requirement is a Sun Ultra 1 running at 143 MHz with 64 MB of DRAM.



### Note

These are only the recommended configurations for running CMS. For information about all supported operating systems, see the next section.

## Operating System and Browser Support

You can access the web-based interfaces by using the operating systems and browsers listed in Table 4. CMS checks the browser version when starting a session to ensure that the browser is supported.

**Table 4 Supported Operating Systems and Browsers**

Operating System	Minimum Service Pack or Patch	Netscape Communicator <sup>1</sup>	Microsoft Internet Explorer <sup>2</sup>
Windows 95	Service Pack 1	4.75, 6.22, or 6.23	5.5 or 6.0
Windows 98	Second Edition	4.75, 6.22, or 6.23	5.5 or 6.0
Windows NT 4.0	Service Pack 3 or later	4.75, 6.22, or 6.23	5.5 or 6.0
Windows 2000	None	4.75, 6.22, or 6.23	5.5 or 6.0
Windows XP	None	4.75, 6.22, or 6.23	5.5 or 6.0
Solaris 2.5.1 or later	Sun-recommended patch cluster for the OS and Motif library patch 103461-24	4.75, 6.22, or 6.23	Not supported

1. Netscape Communicator version 6.0 is not supported.
2. Service Pack 1 or higher is required for Internet Explorer 5.5.



**Note**

If your browser is Internet Explorer and you receive an error message stating that the page might not display correctly because your security settings prohibit running activeX controls, this might mean that your security settings are set too high. To lower security settings, go to **Tools > Internet Options**, and select the **Security** tab. Select the indicated **Zone**, and move the **Security Level for this Zone** slider from **High** to **Medium** (the default).



**Note**

In Cluster Management displays, Internet Explorer versions 4.01 and 5.0 might not display edge devices that are not connected to the command switch. Other functionality is similar to that of Netscape Communicator.

## Supported Java Plug-Ins

One of these Java plug-ins is required for the browser to access and run the Java-based CMS:

- Java plug-in 1.4
- Java plug-in 1.3.1

These Java plug-ins are supported both in Windows environments and on Solaris platforms. You can download the plug-ins and installation instructions from this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/java>



**Note**

Only one of these Java plug-ins is required for CMS. Do not install more than one Java plug-in.

On Solaris platforms, follow the instructions in the README\_FIRST.txt file to install the Java plug-in.

## Java Plug-In Notes

These notes apply to Java plug-in configuration:

- To verify that a supported version of the Java plug-in is installed, select **Start > Settings > Control Panel**. The Java plug-in is listed with the version number in the Control Panel menu.
- If you have installed the Java plug-in but CMS still does not launch, make sure that the plug-in is enabled by selecting **Start > Settings > Control Panel > Java Plug-in**. Click the Basic tab, select Enable Java Plug-in, and click Apply.
- If the Java applet does not initialize after you have installed and enabled the plug-in, open the Java Plug-in Control Panel (**Start > Programs > Java Plug-in Control Panel**), and verify these settings:  
In the Proxies tab, verify that **Use browser settings** is checked and that no proxies are enabled.
- If you are running an Internet virus checker on Windows 2000 and the plug-in takes a long time to load, you can speed up CMS operation by disabling the virus checker filter option or download option or both.

From the Start menu on McAfee VirusScan, disable the VirusScan Internet Filter option, the Download Scan option, or both by selecting **Start > Programs > Network Associates > Virus Scan Console > Configure**.

or

From the taskbar, right-click the Virus Shield icon and in the Quick Enable menu, disable the options by deselecting **Internet Filter** or **Download Scan**. Windows XP, Windows 2000, Windows 95, Windows 98, and Windows NT 4.0 Plug-Ins

## Cluster Capability

When creating a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.

A Catalyst 2950 switch can be a command switch or a member of a switch cluster.

If your cluster has Catalyst 2950, Catalyst 2955, Catalyst 2940, Catalyst 2900 XL, and Catalyst 3500 XL switches, the Catalyst 2950 switch should be the command switch. The Catalyst 2950 switch that has the latest software should be the command switch.

[Table 5](#) lists the cluster capabilities and minimum software versions for the switches. The switches are listed in the order of highest to lowest end switch. A lower-end switch cannot be the command switch of a switch listed above it in the table. For example, a Catalyst 2940 switch cannot be the command switch of a cluster that has Catalyst 2950 or Catalyst 3500 switches.

**Table 5** *Switch Software and Cluster Capability*

Switch	Cisco IOS Release	Cluster Capability
Catalyst 3750	Cisco IOS Release 12.1(11)AX or later	Member or command switch
Catalyst 3550	Cisco IOS Release 12.1(4)EA1 or later	Member or command switch
Catalyst 2970	Cisco IOS Release 12.1(11)AX later	Member or command switch
Catalyst 2955	Cisco IOS Release 12.1(12c)EA1 or later	Member or command switch
Catalyst 2950	Cisco IOS Release 12.0(5.2)WC(1) or later	Member or command switch
Catalyst 2950 LRE	Cisco IOS Release 12.1(11)JY or later	Member or command switch

**Table 5** Switch Software and Cluster Capability (Continued)

Switch	Cisco IOS Release	Cluster Capability
Catalyst 2940	Cisco IOS Release 12.1(13)AY or later	Member or command switch
Catalyst 3500 XL	Cisco IOS Release 12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	Cisco IOS Release 12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	Cisco IOS Release 11.2(8.5)SA6 (recommended)	Member switch only <sup>1</sup>
Catalyst 1900 and 2820	Cisco IOS Release 9.00(-A or -EN)	Member switch only

1. Catalyst 2900 XL (4-MB) switches appear in the front-panel and topology views of CMS. However, CMS does not support configuration or monitoring of these switches.

Some versions of the Catalyst 2900 XL software do not support clustering, and if you have a cluster with switches that are running different versions of software, software features added on the latest release might not be reflected on switches running the older versions. For example, if you start Visual Switch Manager (VSM) on a Catalyst 2900 XL switch running Cisco IOS Release 11.2(8)SA6, the windows and functionality can be different from a switch running Cisco IOS Release 12.0(5)WC(1) or later.



**Note**

The CMS is not forward-compatible, which means that if a member switch is running a software version that is newer than the release running on the command switch, the new features are not available on the member switch. If the member switch is a new device supported by a software release that is later than the software release on the command switch, the command switch cannot recognize the member switch and it is displayed as an unknown device in the Front Panel view. You cannot configure any parameters or generate a report through CMS for that member; instead, you must launch the Device Manager application to perform configuration and obtain reports for that member.

## Downloading Software

This section describes these procedures for downloading software:

- [“Determining the Software Version and Feature Set” section on page 8](#)
- [“Determining Which Files to Use” section on page 8](#)
- [“Upgrading a Switch by Using the CLI” section on page 9](#)
- [“Recovering from Software Failure” section on page 13](#)

For information about the software releases that support the Catalyst 2950 switches, see the [“Limitations and Restrictions” section on page 16](#).



**Note**

Before downloading software, read this section for important information.



**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, refer to the “Recovering from Corrupted Software” section in the “Troubleshooting” chapter of the software configuration guide for this release.



**Note**

---

If you are upgrading a switch that is running a release earlier than Cisco IOS Release 12.1(11)EA1, this release includes a bootloader upgrade. The bootloader can take up to 30 seconds to upgrade.

---



**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, call Cisco Systems immediately.

---

## Determining 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 number. 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.



**Note**

---

Although the **show version** output always shows the software image running on the switch (SI or EI), the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software image.

---

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

## Determining Which Files to Use

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

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



**Note**

---

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.

---

Table 6 lists the software filenames for this Cisco IOS release.

**Table 6** Catalyst 2950 Cisco IOS Software Files

Filename	Description
c2950-i6k2l2q4-tar.121-14.AZ.tar	Catalyst 2950 SI <sup>1</sup> and EI files. This includes the enhanced crypto Cisco IOS image and CMS files.
c2950-i6q4l2-tar.121-14.AZ.tar	Catalyst 2950 SI and EI files. This includes the enhanced and standard Cisco IOS image, and CMS files.

1. Switches that support only the SI cannot run the crypto image. For more information, see the SI-only switches listed in Table 1 and the “Cisco IOS Limitations and Restrictions” section on page 16.

## Upgrading a Switch by Using CMS

You can upgrade switch software by using CMS. From the menu bar, select **Administration > Software Upgrade**. For detailed instructions, click **Help**.



### Note

If you are upgrading a switch that is running a release earlier than Cisco IOS Release 12.1(11)EA1, this release includes a bootloader upgrade. The bootloader can take up to 30 seconds to upgrade.



### Caution

Do not power cycle the switch while you are copying an image to the switch. If a power failure occurs when you are copying the software image to the switch, call Cisco Systems immediately.

## Upgrading a Switch by Using the CLI

To download switch software by using the CLI, follow these procedures in this order:

1. Decide which software files to download from Cisco.com (see the “Determining the Software Version and Feature Set” section on page 8).
2. Download the .tar file from Cisco.com (see the “Downloading the Software” section on page 10).  
Use the **archive tar** command to extract the image and the CMS files from the .tar file during the TFTP copy to the switch. 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.
3. Copy the current startup configuration file (see the “Copying the Current Startup Configuration from the Switch to a PC or Server” section on page 10).
4. If you are using the CLI to upgrade a Catalyst 2950 switch, see the “Using the CLI to Upgrade a Catalyst 2950 Switch” section on page 11.



### Note

If you are upgrading from a Cisco IOS release earlier than Cisco IOS Release 12.1(6)EA2, use the **tar** command instead of the **archive tar** command as described in the “Using the CLI to Upgrade a Catalyst 2950 Switch” section on page 11.

## Downloading the Software

This procedure is for copying the combined .tar file to the Catalyst 2950 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.



### Note

---

If you do not have access to a TFTP server, download it before downloading the software.

---

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

- 
- Step 1** Use [Table 6](#) to identify the files that you want to download.
- Step 2** Download the files from one of these locations:
- If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:  
<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>
  - If you do not have a SmartNet contract, go to this URL, follow the instructions to register on Cisco.com, and download the appropriate files:

<http://www.cisco.com/public/sw-center/sw-lan.shtml>

To download the files, select **Catalyst 2950** for a Catalyst 2950 switch.

To obtain authorization and download the enhanced crypto software files, select **Catalyst 2950 Strong Cryptographic (3DES) Software** for a Catalyst 2950 switch.

- Step 3** 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 PC or server.

This procedure requires a configured TFTP server.

Beginning in privileged EXEC mode, follow these steps to copy a switch configuration file to the PC or server that has the TFTP server application:

- 
- 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 PC or server.
- 

## Using the CLI to Upgrade a Catalyst 2950 Switch

Use this procedure for upgrading Catalyst 2950 switch by copying the .tar file to the switch. You copy the files to the switch from a TFTP server and 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 CMS pages and deletes the existing CMS files before the software upgrade to avoid a conflict if users access the web pages during the software upgrade.
- Re-enables access to the CMS pages after the upgrade is complete.



### Note

If you are upgrading a switch that is running a release earlier than Cisco IOS Release 12.1(11)EA1, this release includes a bootloader upgrade. The bootloader can take up to 30 seconds to upgrade.



### Caution

Do not power cycle the switch while you are copying an image to the switch. If a power failure occurs when you are copying the software image to the switch, call Cisco Systems immediately.

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** Access the CLI 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 CMS files:

```
switch# delete flash:html/*
```

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 CMS files to Flash memory:



**Caution**

In this step, the **archive tar** command copies the .tar file that contains both the image and the CMS 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.EA1b.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.EA1b.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 resets.

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 CMS files.

---

## Recovering from Software Failure

If the software fails, you can reload the software. For detailed recovery procedures, refer to the “Troubleshooting” chapter in the software configuration guide for this release.

## Installation Notes

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

- The Express Setup program if your Catalyst 2950 switch is running Cisco IOS Release 12.1(14)EA1 or later (Refer to the *Catalyst 2950 Switch Hardware Installation Guide*.)
- The CLI-based setup program (See the [“Setting Up the Catalyst 2950 Switch Initial Configuration” section on page 13.](#))
- The Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration (Refer to the *Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*.)
- Manually assigning an IP address (Refer to the *Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*.)

## Setting Up the Catalyst 2950 Switch Initial Configuration

The first time that you access the switch, it runs a setup program that prompts you for an IP address and other configuration information necessary for the switch to communicate with the local routers and the Internet. This information is also required if you plan to use the CMS to configure and manage the switch.



### Note

If the switch will be a cluster member managed through the IP address of the command switch, it is not necessary to assign IP information or a password. If you are configuring the switch as a standalone switch or as a command switch, you must assign IP information.

---

Follow these steps to create an initial configuration for the switch:

**Step 1** Enter **Yes** at the first two prompts.

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system.

```
Would you like to enter basic management setup? [yes/no]: yes
```

**Step 2** Enter a host name for the switch, and press **Return**.

On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters.  
Do not use *-n*, where *n* is a number, as the last character in a host name for any switch.

```
Enter host name [Switch]: host_name
```

**Step 3** Enter a secret password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive,  
allows spaces, but ignores leading spaces.

```
Enter enable secret: secret_password
```

**Step 4** Enter an enable password, and press **Return**.

```
Enter enable password: enable_password
```

**Step 5** Enter a virtual terminal (Telnet) password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores  
leading spaces.

```
Enter virtual terminal password: terminal-password
```

**Step 6** (Optional) Configure the Simple Network Management Protocol (SNMP) by responding to the prompts.

**Step 7** Enter the interface name (physical interface or VLAN name) of the interface that connects to the  
management network, and press **Return**. For this release, always use VLAN 1 as that interface.

```
Enter interface name used to connect to the  
management network from the above interface summary: vlan 1
```

**Step 8** Configure the interface by entering the switch IP address and subnet mask and pressing **Return**:

```
Configuring interface vlan1:  
Configure IP on this interface? [yes]: yes  
IP address for this interface: 10.4.120.106  
Subnet mask for this interface [255.0.0.0]: 255.255.255.0
```

**Step 9** Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member  
switch or as a standalone switch.

If you enter **N**, the switch appears as a candidate switch in the CMS. In this case, the message in [Step 10](#)  
does not appear.

```
Would you like to enable as a cluster command switch? [yes/no]: yes
```

**Step 10** Assign a name to the cluster, and press **Return**.

```
Enter cluster name: cluster_name
```

The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

The initial configuration appears:

The following configuration command script was created:

```
hostname host_name
enable secret 5 $1$Max7$Qgr9eXBhtcBJw3KK7bc850
enable password my
line vty 0 15
password my_password
snmp-server community public
!
no ip routing
!
interface Vlan1
no shutdown
ip address 172.20.139.145 255.255.255.224
!
interface Vlan2
shutdown
no ip address
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
...<output abbreviated>
!!!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
end
```

**Step 11** These choices appear:

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

```
Enter your selection [2]:
```

Make your selection, and press **Return**.

---

After you complete the setup program, the switch can run the created default configuration. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- CLI
- CMS from your browser

# New Features

For a list of supported hardware, see the [“Hardware Supported” section on page 2](#). These are the new features for the Catalyst 2950SX-48-SI and 2950T-48-SI switches:

- The Catalyst 2950SX-48-SI and 2950T-48-SI both support the standard image (SI).



---

**Note** For more information about features supported by the SI, refer to the switch software configuration guide for Cisco IOS Release 12.1(14)EA1.

---

- The 10/100/1000 ports on the Catalyst 2950T-48-SI switch operate at 10 or 100 Mbps in either full- or half-duplex mode or at 1000 Mbps only in full-duplex mode.
- The 1000BASE-SX ports on the Catalyst 2950SX-48-SI switch operate only at 1000 Mbps and in full-duplex mode.
- You can configure the speed on Fast Ethernet (10/100 Mbps) and Gigabit Ethernet (10/100/1000 Mbps) interfaces. You cannot configure the speed on the 100BASE-FX, 1000BASE-SX, GBIC-module, and SFP module interfaces.
- You can configure the duplex mode on any Fast Ethernet interfaces that are not set to autonegotiate. You can configure the duplex mode on the 10/100/1000 ports on the Catalyst 2950T-48-SI switch.

# 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 2950 switches unless otherwise noted.

---

These are the limitations and restrictions:

- [“Cisco IOS Limitations and Restrictions” section on page 16](#)
- [“CMS Limitations and Restrictions” section on page 21](#)
- [“Cluster Limitations And Restrictions” section on page 23](#)
- [“Hardware and Software Compatibility Matrixes” section on page 23](#)

# 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.  
There is no workaround. (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.  
There is no workaround. (CSCdr96565)

- 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 obtain its IP address from the dynamic pool. (CSCds58369)

- 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.

There is no workaround. (CSCds20365)

- 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.

There is no workaround. (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.

There is no workaround. (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.

There is no workaround. (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 802.1X port to be de-authenticated.

The workaround is to manually re-initiate authentication by either logging off or detaching the link and then re-connecting 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.

There is no workaround. (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 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 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 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 2940, Catalyst 2950, or Catalyst 2955 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.

There is no workaround. (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, refer to 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 crypto software image, your switch configuration must meet these conditions:
  - The number of trunk ports multiplied by the number of VLANs on the switch must be less than or equal to 128. These are examples of switch configurations that meet this condition:  
If the switch has 2 trunk ports, it can have up to 64 VLANs.  
If the switch has 32 VLANs, it can have up to 4 trunk ports.
  - If your switch is a cluster command switch, it can only support up to eight cluster members.



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

If your switch has a saved configuration that does not meet the previous conditions and you upgrade the switch software to the crypto 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 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. (CSCdy38476)

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.
- 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.

There is no workaround. (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.

There is no workaround. (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 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. (CSCea12888)

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
```
- Telnet 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.

- 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 a switch sends a system message to an external syslog server, the switch adds a sequence number to the system message. (CSCea26598)
- 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 transition 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.

There is no workaround. (CSCea47230)

## CMS Limitations and Restrictions

These limitations apply to CMS configuration:

- A red border appears around the text-entering area of some CMS dialogs. The color of the border changes to green when text is entered. This is only a cosmetic error. The colored border does not prevent you from entering text.

There is no workaround. (CSCdv82352)




---

**Note** This error only occurs with Java plug-in 1.4.0.

---

- You cannot switch modes (for example, from Guide Mode to Expert Mode) for an open CMS window.

The workaround is to close the open window, select the mode that you want, and then reopen the CMS window. (CSCdw87550)




---

**Note** For the mode change to take effect on any other CMS window that is open, you need to close that window and then reopen it after you select the new mode.

---

- After you click Apply or Refresh in the SNMP window, the window size changes.

There is no workaround. (CSCdz75666)

- When you enable log scaling for Link Graphs, the Y-axis scale becomes illegible.  
There is no workaround. (CSCdz81086)
- The CMS window does not return to full size after resizing the NE or IE when using Netscape version 6.xx on Solaris and Linux. This is a Netscape browser problem.  
There is no workaround. (CSCea01179)
- The CMS files that are downloaded from the switch to your PC or terminal are not cached on the PC or terminal. The files are then downloaded again when CMS is relaunched.  
There is no workaround. (CSCea27601)
- If you launch CMS by using Netscape 4.75 and Java Runtime Environment (JRE) 1.3.1 or 1.4.0 on Windows 98 or by using Netscape 6.2 and JRE 1.3.1 on Windows 98, CMS stops running while it determines the network information.  
The workaround is to click once outside of the CMS window. (CSCea25913)
- On the Japanese versions of Windows 98 and Windows ME, if you launch CMS by using the Netscape 4.7 browser, CMS might stop running after you click the Apply button.  
The workaround is to use Netscape 6.0 or later or use Internet Explorer to launch CMS on Windows 98 and Windows ME. (CSCea27408)
- The icons on the tool bar are blank when you unlock the PC while CMS is running or you interrupt the screen saver on your PC.  
The workaround is to resize the CMS window so that the window is refreshed correctly. (CSCea80753)
- If you change the password or start the authentication process while CMS is running, HTTP requests sent by the switch fail.  
The workaround is to close all browser sessions and then relaunch CMS. (CSCeb33995)
- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when also entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.
- ACEs that contain the **host** keyword precede all other access control entries (ACEs) in standard ACLs. You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.
- Certain combinations of port features create configuration conflicts (see [Table 7](#) for the port configuration conflicts). If you try to enable incompatible features, a warning message appears in CMS, and you cannot make the change. Reload the page to refresh CMS.  
In [Table 7](#), *No* means that the two referenced features are incompatible, and both should not be enabled at the same time; *Yes* means that both can be enabled at the same time and do not cause an incompatibility conflict. A dash means not applicable.

**Table 7**     *Conflicting Features*

	Port Group	Port Security	SPAN Source Port	SPAN Destination Port	Connect to Cluster?	Protected Port	802.1X Port
Port Group	–	No	Yes	No	Yes	Yes	No
Port Security	No	–	Yes	No	Yes	Yes	Yes <sup>1</sup>
SPAN Source Port	Yes	Yes	–	No	Yes	Yes	Yes
SPAN Destination Port	No	No	No	–	Yes	Yes	No
Connect to Cluster	Yes	Yes	Yes	Yes	–	Yes	–
Protected Port	Yes	Yes	Yes	Yes	Yes	–	–
802.1X Port	No	Yes <sup>1</sup>	Yes	No	–	–	–

1. The switch must be running the EI.

## Cluster Limitations And Restrictions

This limitation and restriction applies to the cluster configuration:

- When a cluster of switches have NTP (Network Time Protocol) configured, the command switch is not synchronized with the rest of the switches.

There is no workaround. (CSCdz88305)

## Hardware and Software Compatibility Matrixes

Some 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 2950SX-48-SI and 2950T-48-SI switches are supported by Cisco IOS Release 12.1(14)AZ or later.

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

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

**Table 8 Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches (Continued)**

Hardware	Serial Number	Cisco IOS Release 12.0(5)WC2b or Earlier	Cisco IOS Release 12.1(6)EA2, Cisco IOS Release 12.1(6)EA2a, and Cisco IOS Release 12.1(6)EA2b	Cisco IOS Release 12.1(6)EA2c	Cisco IOS Release 12.1(9)EA1 or Later
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

## Important Notes



Note

These important notes apply to all Catalyst 2950 switches unless otherwise noted.

This section describes important information related to this release. These sections are included:

- [“Cisco IOS Notes” section on page 25](#)
- [“CMS Notes” section on page 26](#)

## Cisco IOS Notes

These notes applies to Cisco IOS configuration:

- 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 IP phone 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 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. Refer to the *Catalyst 2950 and Catalyst 2955 Switch Command Reference* for information about using the **shutdown** interface configuration command.

- When an 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 transition to the unauthorized state. If this happens, it can take up to 60 minutes for the interface to transition 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 802.1X client, not with the switch.

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

```
dot1x timeout quiet-period 3
dot1x timeout tx-period 5
```

## CMS Notes

These notes apply to the CMS configuration:

- If you use CMS on Windows 2000, it might not apply configuration changes if the enable password is changed from the CLI during your CMS session. You have to restart CMS and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- If you have a proxy server configured on your web browser, CMS can run slowly and take 2 to 3 minutes to process each command that is entered.

The workaround, if you do not want to disable the proxy server settings on the browser, is to download a browser from a different vendor and use it without the proxy server settings configured to access the CMS.

- CMS does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using CMS, you cannot create classes that match more than one match statement. CMS does not display policies that have such classes.
- 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 CMS.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.
- In the Front Panel view or Topology view, CMS does not display error messages in read-only mode for these switches:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

In the Front Panel view, if the switch is running one of the software releases listed previously, the device LEDs do not appear. In Topology view, if the member is an LRE switch, the CPE devices that are connected to the switch do not appear. The Bandwidth and Link graphs also do not appear in these views.

# Open Caveats



Note

---

These important notes apply to all Catalyst 2950 switches unless otherwise noted.

---

These are the open caveats in this release:

- [“Open Cisco IOS Caveats” section on page 27](#)
- [“Open CMS Caveats” section on page 30](#)

## Open Cisco IOS Caveats

These are the open Cisco IOS configuration caveats:

- CSCea87794

When MAC addresses are learned and deleted at high rates on a switch, addresses on dynamic access ports might need to be authenticated again from the VLAN Membership Policy Server (VMPS), causing traffic to drop until authentication is complete.

The workaround is to reduce the MAC address learning and MAC address movement activity.

- CSCeb36925

A FastEthernet port that has been configured at 10 Mbps might stay linked up or link flap after the device to which is have been linked to has been shut down.

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

- CSCeb55987

When UplinkFast is configured on a Catalyst 2950 or Catalyst 3550 switch, the MAC address of the switch is not forwarded to the uplink switch through the new link. This temporarily interrupts communication with the management VLAN and delays convergence of UplinkFast.

There is no workaround.

- CSCec13986

After a topology change in Spanning Tree Protocol (STP) occurs, 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 the management VLAN, this failure does not occur.

---

The workaround is to place the ports in static-access mode for a single VLAN, if possible, in the topology.

- CSCdz43526

When you use the **show vlan** user EXEC command and VLANs are added in VTP Transparent mode, the switch displays this traceback message:

```
*Mar  2 19:06:39: %SYS-3-CPUHOG: Task ran for 2016 msec (3/2), process = Exec, PC =
801E9628. -Traceback= 801E9630 8013F5B8 8013F9BC 8014B164 8014AA54 8014A9AC 8016CB78
801D3544 801D3530 ctnwa303#
```

There is no workaround. This does not affect the functionality of the switch.

- CSCec00317

When the STP state changes to blocking on a Catalyst 2950 switch that is running Cisco IOS Release 12.1(14)EA1, the status LED does not turn amber.

There is no workaround.

- CSCec07477

When a Catalyst 2950 switch is running Cisco IOS Release 12.1(13)EA1 or 12.1(14)EA1, the switch fails when it receives a *get next request* SNMP packet.

The workaround is to remove the switch sending the *get next request* SNMP packet from the network.

- CSCec29265

A Catalyst 2950 switch running 12.1(14)EA1 could fail when the service assurance agent (SAA) is configured by using the internetwork performance monitor (IPM) CiscoWorks2000 application.

The workaround is to use the CLI to configure SAA.

- CSCec35710

If you configure storm control and port security on all 48 ports of a Catalyst 2950SX-48-SI or a 2950T-48-SI switch running Cisco IOS Release 12.1(14)AZ and configure a VLAN interface, the switch returns an error message.

The workaround is to configure storm control and port security on 24 or fewer ports.

- CSCdx75308

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.

- CSCdx95501

When a community string is assigned by the cluster command switch, you cannot get any dot1dBridge MIB objects 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
```

- CSCea63436

When a Catalyst 2950 running the c2950-i6q412-mz.121-13.EA1.bin software image is running Multicast VLAN Registration (MVR) dynamic mode, the source port MVR membership flaps.

The workaround is to enter the **no ip igmp snooping report-suppression** interface configuration command, which was introduced in Cisco IOS Release 12.1(14)EA1.

- CSCea69056

When 10/100 Mbps ports are connected to one another through media converters and 100BASE-FX media, the link fails.

There is no workaround.

- CSCeb05425

If you configure an ACL such that a DHCP server allocates a specific IP address and configuration information on an interface, such as this ACL:

```
access-list 104 permit ip host 192.5.0.0 any
access-list 104 permit ip host 0.0.0.0 any
```

The switch does not apply the ACL to the interface.

The field sets of all the ACEs in an ACL on Ethernet interface should match. Refer to the software configuration guide to understand mask restrictions for ACLs on Ethernet interfaces.

The workaround is to configure the host with a static IP address and configure the DHCP server to not allocate an IP address to the host.

- CSCeb05733

When an LACP channel group with hot standby ports is restarted by using the **shutdown** and **no shutdown** interface configuration commands, this error message appears:

```
%SM-4-BADEVENT: Event 'link_down' is invalid for the current state 'link_down':
```

There is no workaround.

- CSCeb33988

If too many traps are enabled when a switch powers on, it might not generate the coldStart trap.

There is no workaround.

- CSCeb47201

After clearing the MAC address table on a Catalyst 2950G-48 running 12.1(13)EA1b, an ICMP echo\_request is not sent from one port channel to another port.

There is no workaround.

- CSCeb49033

Under the following conditions, configuring **mac-address-table notification** can cause the switch to run out of memory and fail. Using **mac-address-table notification history-size** and **mac-address-table notification interval** to tune the process does not resolve the problem.

- Large number of MAC address flapping

With the wrong setup, a single host with multiple NICs can be connected to the switch by using the same MAC address in the same VLAN. As the result, the MAC address flaps from port to port generating many *adds* and *drops* from the MAC address table.

- MAC address flooding attack

With a MAC address flooding attack, a single NIC host sends out many packets with different source MAC addresses, which also generates many *adds* for the MAC address table.

The workaround for the first case is to turn off the MAC address table notification, and the workaround for the second case is to use port security to inhibit the attack.

- CSCeb55987

When UplinkFast is configured on a Catalyst 2950 or Catalyst 3550 switch, the MAC address of the switch is not forwarded to the uplink switch through the new link. This temporarily interrupts communication with the management VLAN and delays convergence of UplinkFast.

There is no workaround.

- CSCeb61370

If a Cisco Catalyst WS-2950G-48-EI switch that is running the cryptographic image has the maximum number of supported 128 virtual ports (number of trunk ports multiplied by the number of VLANs) and is also the switch master, the **show running-configuration** privileged EXEC command might fail, or a memory fragmentation error message might appear.

The workaround is to reduce memory usage by removing unused configurations. For example, use another switch in the cluster as the switch master, or remove unused VLANs.

- CSCeb62247

With light Layer 2 multicast traffic (about 10 mbps line rate), IP IGMP query messages might fail to reach the Catalyst 2950, which causes the IP IGMP snooping feature to fail.

The workaround is to disable source-only-learning or stop multicast traffic.

## Open CMS Caveats

These are the open CMS configuration caveats:

- CSCdz01037

CMS does not work when a switch is running the crypto software image and the vty lines are configured to use only SSH by using the **transport input ssh line vty 0 15** interface configuration command.

The workaround is to allow SSH and Telnet access through the vty lines by using the **transport input ssh telnet** interface configuration command.

- CSCdz15119

If only one management VLAN interface is configured on a switch, you cannot change the management VLAN interface to another management VLAN interface by using CMS.

The workaround is to create a second management VLAN interface before you use CMS to change the management interface.

- CSCdz23548

When you use Visual Switch Manager (VSM) to configure Catalyst 2900 XL and Catalyst 3500 XL switches, the configuration is not saved if you save it in VSM.

The workaround is to save the configuration by using the CLI.

- CSCeb05183

On the Catalyst 2820 and Catalyst 1900 switches, the Port Settings table might show incorrect information in the interface description and duplex columns.

There is no workaround.

- CSCeb11990

On a switch running Cisco IOS Release 12.1 or later, the Bridge Parameter tab in the STP window incorrectly shows IBM as an STP bridge protocol option. This option is no longer supported on the switch.

There is no workaround.
- CSCeb23334

On a switch running Cisco IOS Release 12.1 or later, CMS does not validate STP port-priority configuration values before they are added to the switch configuration. When these invalid values are added to the switch configuration, an error message does not appear.

There is no workaround.
- CSCeb23416

On a switch running Cisco IOS Release 12.1 or later, CMS does not validate STP port-path-cost configuration values before they are added to the switch configuration. When these invalid values are added, an error message does not appear.

There is no workaround.
- CSCeb23592

On a switch running Cisco IOS Release 12.1 or later, CMS does not validate STP bridge-parameter values before they are added to the switch configuration. When these invalid values are added, an error message does not appear.

There is no workaround.
- CSCeb25630

The Link Graphs bar chart for Packet Drops and Errors might display incorrect information about the Ethernet interfaces.

The workaround is to use the **show interfaces** or **show interfaces counter** privileged EXEC command.
- CSCeb38514

If one of the stack members goes down or a stack member is disconnected from the stack, a stack icon might disappear from the topology view.

The workaround is to close the CMS browser and to relaunch CMS.
- CSCeb38676

If you are launching CMS in read-only mode, Java exceptions might occur. These exceptions do not affect the CMS functionality.

There is no workaround.
- CSCeb38967

When CMS is in read-only mode, an error message appears if the online Help is launched from the QoS Graph window.

There is no workaround.

- CSCeb40625

Shaped bandwidth weights are invalid if the sum of their reciprocals is greater than 1 and the weight of a queue is zero. CMS does not configure these invalid bandwidth weights.

There is no workaround.

## Documentation Updates

You can access all Catalyst 2950 documentation at this URL:

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

## Correction to the Catalyst 2950 Switch Hardware Installation Guide

The “Quick Setup” chapter states that the Express Setup program is supported on Catalyst 2950 LRE switches running Cisco IOS Release 12.1(14)EA1 or later. Express Setup is only supported on Catalyst 2950 LRE switches running Cisco IOS Release 12.1(19)EA1 or later.

## Corrections to the Software Configuration Guide and Command Reference

These are corrections for the *Catalyst 2950 Desktop Switch Software Configuration Guide* and *Catalyst 2950 Desktop Switch Command Reference*:

- The information about the duplex mode of the 10/100/1000 ports on the Catalyst 2950T-24 switch is incorrect in the software configuration guide and command reference.  
You can configure a 10/100/1000 port to autonegotiate the duplex mode or manually set the duplex mode to full by using the **duplex {auto | full}** interface configuration command. The 10/100/1000 interfaces on the Catalyst 2950T-24 switch do not support the **half** keyword in the duplex command.
- The command syntax for the **udld** interface configuration command is incorrect in the command reference and the software configuration guide. The correct syntax is **udld port [aggressive | disable]**; the syntax and usage guidelines incorrectly include the **enable** option. Also, the usage guidelines should use **udld port**, not just **udld**, when referring to this command.
- The **ip igmp snooping report-suppression** global configuration command was omitted from the command reference for this release.

## ip igmp snooping report-suppression

Use the **ip igmp snooping report-suppression** global configuration command to enable IGMP report suppression. Use the **no** form of this command to disable IGMP report suppression and forward all IGMP reports to multicast routers.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

**Syntax Description** This command has no arguments or keywords.

**Defaults** IGMP report suppression is enabled.

**Command Modes** Global configuration

Release	Modification
12.1(14)EA1	This command was introduced.

**Usage Guidelines** When IGMP report suppression is enabled, the switch sends only one IGMP report per multicast router query to the multicast devices. The switch sends the first IGMP report from all hosts for a group to all the multicast routers and does not send the remaining IGMP reports to the multicast routers. If a mulitcast router query includes requests for IGMPv1 and IGMPv2 reports, the switch sends both types of reports. IGMP report suppression prevents duplicate reports from being sent to the multicast devices. If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all the multicast routers.



**Note** Though the **tcn** keyword is visible in the command-line help string, the **ip igmp snooping tcn** command is not supported.

**Examples** This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

This example shows how to enable report suppression:

```
Switch(config)# ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Command	Description
<b>ip igmp snooping</b>	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
<b>show ip igmp snooping</b>	Displays the IGMP snooping configuration of the switch or the VLAN.

## Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

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

The software documents are not shipped with the product, but you can access them under the appropriate Cisco IOS software release on Cisco.com. 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 34.

These publications provide more information about the switches:

- *Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)
- *Catalyst 2955 Hardware Installation Guide* (order number DOC-7814944=)
- *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=)

## Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

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

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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.

## Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

## Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

## Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)

---

This document is to be used with the documentation listed in the “[Related Documentation](#)” section.



Copyright © 2003 Cisco Systems, Inc. All rights reserved.