



Release Notes for the Catalyst 2950 Desktop Switch, Release 12.1(11)EA1a

October 2002

The Cisco IOS Release 12.1(11)EA1a runs on Catalyst 2950 switches.

These release notes include important information about this IOS 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 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 IOS version.

For the complete list of Catalyst 2950 switch documentation, see the [“Related Documentation” section on page 41](#).

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

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 18](#)
- [“New Software Features” section on page 21](#)
- [“Limitations and Restrictions” section on page 21](#)
- [“Important Notes” section on page 25](#)
- [“Open Caveats” section on page 27](#)
- [“Resolved Caveats” section on page 35](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

- [“Documentation Updates” section on page 37](#)
- [“Related Documentation” section on page 41](#)
- [“Obtaining Documentation” section on page 41](#)
- [“Obtaining Technical Assistance” section on page 42](#)

System Requirements

These are the system requirements for this IOS release:

- [“Hardware Supported” section on page 2](#)
- [“Hardware Not Supported” section on page 3](#)
- [“Software Compatibility” section on page 3](#)

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).

For information about the software releases that support the switches listed in [Table 1](#), see the [“Limitations and Restrictions” section on page 21](#).

[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 ¹ 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 ²

Table 1 *Hardware Supported (continued)*

Hardware	Software Image	Description
GBIC Modules	—	<ul style="list-style-type: none"> • 1000BASE-SX GBIC • 1000BASE-LX/LH GBIC • 1000BASE-ZX GBIC • 1000BASE-T GBIC (model WS-5483) • Coarse Wave Division Multiplexer (CWDM) fiber-optic GBIC³ • GigaStack GBIC
Redundant power system	—	Cisco RPS 300 Redundant Power System

1. GBIC = Gigabit Interface Converter
2. The 10/100/1000 ports operate only in full-duplex mode.
3. 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-G4582)
Redundant power system	Cisco RPS 600 Redundant Power System

Software Compatibility

These are the software compatibility requirements for this IOS release:

- [“Recommended Platform Configuration for Web-Based Management”](#) section on page 4
- [“Operating System and Browser Support”](#) section on page 4
- [“Installing the Required Plug-In”](#) section on page 5
- [“Creating Clusters with Different Releases of IOS Software”](#) 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 ¹	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.

For information about 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. The switch checks the browser version when starting a session to ensure that the browser is supported. If the browser is not supported, the switch displays an error message, and the session does not start.

Table 4 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Netscape Communicator ¹	Microsoft Internet Explorer ²
Windows 95	Service Pack 1	4.75 or 6.2	5.5 or 6.0
Windows 98	Second Edition	4.75 or 6.2	5.5 or 6.0
Windows NT 4.0	Service Pack 3 or later	4.75 or 6.2	5.5 or 6.0
Windows 2000	None	4.75 or 6.2	5.5 or 6.0
Windows XP	None	4.75 or 6.2	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 or 6.2	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.

Installing the Required Plug-In

A Java plug-in is required for the browser to access and run the Java-based Cluster Management Suite (CMS). Download and install the plug-in before you start CMS. Each platform, Windows and Solaris, supports three plug-in versions. For information on the supported plug-ins, see the “[Windows XP, Windows 2000, Windows 95, Windows 98, and Windows NT 4.0 Plug-Ins](#)” section on page 5 and the “[Solaris Plug-Ins](#)” section on page 6.

You can download the recommended plug-ins from this URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/java>

**Note**

Uninstall any older versions of the Java plug-ins before installing the new Java plug-in.

If the Java applet does not initialize after you have installed 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 the **Use browser settings** is checked and that no proxies are enabled.

**Note**

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.

On McAfee VirusScan, from the Start menu, to disable the VirusScan Internet Filter option, the Download Scan option, or both, select **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

These Java plug-ins are supported in the Windows environments:

- Java plug-in 1.4
- Java plug-in 1.3.1
- Java plug-in 1.3.0

You can download these plug-ins from this URL:

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

**Note**

If you start CMS without having installed the required Java plug-in, the browser automatically detects this. If you are using a supported Internet Explorer browser, it automatically downloads and installs the Java plug-in 1.4 (default). If you are using a supported Netscape browser, the browser displays a Cisco.com page that contains the Java plug-in and installation instructions. If you are using Windows 2000, Netscape Communicator might not detect the missing Java plug-in.

Solaris Plug-Ins

These Java plug-ins are supported on the Solaris platform:

- Java plug-in 1.4
- Java plug-in 1.3.1
- Java plug-in 1.3.0

You can download these plug-ins and instructions from this URL:

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

To install the Java plug-in, follow the instructions in the README_FIRST.txt file.

Creating Clusters with Different Releases of IOS Software

When a cluster consists of Catalyst 3550 switches and a mixture of other Catalyst switches, we strongly recommend using only the Catalyst 3550 switches as the command and standby command switches. When the command switch is a Catalyst 3550 switch, all standby command switches must also be Catalyst 3550 switches. The Catalyst 3550 switch that has the latest software should be the command switch.

If your cluster has Catalyst 2950, 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.

If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch. The Catalyst 2900 or 3500 XL switch that has the latest software should be the command switch.

Table 5 lists the cluster capabilities and software versions for the switches.

Table 5 *Switch Software and Cluster Capability*

Switch	IOS Release	Cluster Capability
Catalyst 3550	Release 12.1(4)EA1 or later	Member or command switch
Catalyst 3500 XL	Release 12.0(5.1)XU or later	Member or command switch
Catalyst 2950	Release 12.0(5.2)WC(1) or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	Release 12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	Release 11.2(8.5)SA6 (recommended)	Member switch only ¹
Catalyst 1900 and 2820	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 IOS 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 Release 11.2(8)SA6, the windows and functionality can be different from a switch running 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:

- [“Guidelines for Downloading Switch Software” section on page 7](#)
- [“Determining the Software Version and Feature Set” section on page 8](#)
- [“Which Files to Use” section on page 8](#)
- [“Upgrading a Switch by Using CMS” section on page 9](#)
- [“Upgrading a Switch by Using the CLI” section on page 10](#)
- [“Recovering from Software Failure” section on page 18](#)

For information about the software releases that support the Catalyst 2950 switches, see the [“Limitations and Restrictions” section on page 21](#).



Note

Before downloading software, read this section for important information.



Note

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

Guidelines for Downloading Switch Software

When using CMS to upgrade multiple switches from the Cisco TFTP server, the Cisco TFTP server application can process multiple requests and sessions. When using CMS to upgrade multiple switches from the Cisco TFTP server, you must first disable the **TFTP Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.

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 *Catalyst 2950 Desktop Switch Software Configuration Guide*.



Caution

This software release includes a bootloader upgrade. Do not power cycle the switch while you are copying this image to the switch. If a power failure occurs when you are copying the software image to the switch, call Cisco Systems immediately.

Determining the Software Version and Feature Set

The IOS image is stored as a *.bin* file in a directory that is named with the IOS release. A subdirectory contains the HTML 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.

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 IOS image file and the HTML files (needed for the CMS). 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 Release 12.1(6)EA2, use the **tar** command instead of the **archive tar** command.

Table 6 lists the software filenames for this IOS release.

Table 6 Catalyst 2950 Cisco IOS Software Files

Filename	Description
c2950-i6q4l2-mz.121-11.EA1a.bin	Catalyst 2950 SI and EI files
c2950-i6q4l2-tar.121-11.EA1a.tar	Catalyst 2950 SI, EI, and CMS files

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**.

If you are using Cluster Manager to upgrade a switch cluster, you can use the Software Upgrade feature to upgrade all or some of the switches in a cluster at once. Consider these conditions when doing an upgrade:

- You cannot upgrade Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches at the same time. However, you can group together and upgrade Catalyst 1900 and Catalyst 2820 switches at the same time.
- Upgrade Catalyst 1900 and Catalyst 2820 switches last. To function efficiently, these switches need to be rebooted shortly after the upgrade occurs. If you do not click **Reboot Cluster** in 30 seconds after the upgrade, the Catalyst 1900 and Catalyst 2820 switches automatically reboot.
- For Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches, enter the *image_name.tar* filename in the New File Name field. The .tar file contains both the IOS image and the web-management code.
- For Catalyst 1900 and Catalyst 2820 switches, enter the *image_name.bin* filename in the New File Name field. The .bin file contains the software image and the web-management code.

Follow these steps to use Cluster Manager to upgrade software. Refer to the online help for more details.

-
- Step 1** In Cluster Manager, select **Administration > Software Upgrade** to display the Software Upgrade window.
 - Step 2** Enter the .tar filename (for Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches) or the .bin filename (for Catalyst 1900 and Catalyst 2820 switches) that contains the switch software image and the web-management code.

You can enter just the filename or a pathname into the **New Image File Name** field. You do not need to enter a pathname if the image file is in the directory that you have defined as the TFTP root directory.



Caution

This software release includes a bootloader upgrade. Do not power cycle the switch while you are copying this image to the switch. If a power failure occurs when you are copying the software image to the switch, call Cisco Systems immediately.



Note

You can also use Device Manager to upgrade a single switch by following the same software upgrade procedure.



Note

Close your browser after the upgrade process is complete.

Upgrading a Switch by Using the CLI

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

- Decide which software files to download from Cisco.com (see the [“Determining the Software Version and Feature Set”](#) section on page 8).
- Download the .tar file from Cisco.com (see the [“Downloading the Software and TFTP Server Application”](#) section on page 11).

Use the **archive tar** command to extract the IOS image and the HTML files from the .tar file during the TFTP copy to the switch. If you are upgrading from a release earlier than Release 12.1(6)EA2, use the **tar** command instead of the **archive tar** command.

- Copy the current startup configuration file (see the [“Copying the Current Startup Configuration from the Switch to a PC or Server”](#) section on page 11).

If the upgrade to the new software fails or if the new startup configuration fails, you can reinstall the previous version of the switch software and use the copy of the startup configuration file to start the switch. If a failure occurs while copying a new image to the switch, and the old image has already been deleted, see the [“Guidelines for Downloading Switch Software”](#) section on page 7.

- 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 12.
- If you are using the CLI to upgrade a member switch in a switch cluster, follow one of these procedures:
 - If you are upgrading Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL member switches, see the [“Upgrading Catalyst 2950, Catalyst 2900 XL, or Catalyst 3500 XL Member Switches”](#) section on page 15.
 - If you are upgrading Catalyst 1900 or Catalyst 2820 member switches, see the [“Upgrading Catalyst 1900 or Catalyst 2820 Member Switches”](#) section on page 17.

If you are upgrading a member switch in a switch cluster, because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch.



Note

If you are upgrading from an IOS release earlier than 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 12, the [“Upgrading Catalyst 2950, Catalyst 2900 XL, or Catalyst 3500 XL Member Switches”](#) section on page 15, and the [“Upgrading Catalyst 1900 or Catalyst 2820 Member Switches”](#) section on page 17.

Downloading the Software and TFTP Server Application

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.

Follow these steps to download the software and, if necessary, the TFTP server application, 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 **Download Cisco Catalyst 2950 software**.
- 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.
- The readme.txt file describes how to download the TFTP server application. 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 such as the Cisco TFTP server available on Cisco.com.

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

This procedure is for upgrading Catalyst 2950 switches 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 HTML pages and deletes the existing HTML files before the software upgrade to avoid a conflict if users access the web pages during the software upgrade.
- Reenables access to the HTML pages after the upgrade is complete.



Caution

This software release includes a bootloader upgrade. Do not power cycle the switch while you are copying this 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 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 5** If there is no software image defined in the BOOT path-list, enter **dir flash:** to display the contents of Flash memory.
- Step 6** Using the exact, case-sensitive name of the .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with .bin. The image filename is then the same as the downloaded filename but with a .bin extension. This step does not affect the operation of the switch.



Note Perform this step only if you have space available on your switch and want to retain a copy of the old image.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename flash:c2950-i6q412-mz.121-9.EA1.bin flash:c2950-i6q412-mz.121-11.EA1.bin
```

- Step 7** Display the contents of Flash memory to verify the renaming of the file:

```
switch# dir flash:

Directory of flash:/
 3  drwx      10176   Mar 01 2001 00:04:34  html
 6  -rwx       2343   Mar 01 2001 03:18:16  config.text
171 -rwx     1667997   Mar 01 2001 00:02:39  c2950-i6q412-mz.121-11.EA1.bin
 7  -rwx       3060   Mar 01 2001 00:14:20  vlan.dat
172 -rwx        100   Mar 01 2001 00:02:54  env_vars

7741440 bytes total (4788224 bytes free)
```

- Step 8** Enter global configuration mode:

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

- Step 9** 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.121-11.EA1.bin
```



Note If the **show boot** command entered in [Step 4](#) 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 10** Return to privileged EXEC mode:

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

- Step 11** Remove the HTML files:

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

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

Step 12 Enter this command to copy the new image and HTML files to Flash memory:



Caution

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

```
switch# archive tar /x tftp://server_ip_address/path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (110 bytes)
extracting c2950-i6q4l2-mz.121-11.EA1.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 13 Enter global configuration mode:

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

Step 14 Return to privileged EXEC mode:

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

Step 15 Reload the new software with this command:

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

Step 16 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 HTML files.

Upgrading Catalyst 2950, Catalyst 2900 XL, or Catalyst 3500 XL Member Switches



Caution

This software release includes a bootloader upgrade. The bootloader can take up to 30 seconds to upgrade. Do not power cycle the switch while you are copying the software image to the switch. If a power failure occurs when you are copying the image to the switch, call Cisco Systems immediately.

Follow these steps to upgrade the software on a member switch:

Step 1

In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the output, select the number of the member switch that you want to upgrade. The member number is in the SN column of the display. You need this member number for Step 2.

Step 2

Log in to the member switch (for example, member number 1):

```
switch# rcommand 1
```

Step 3

Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

Step 4

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
Private Config file: flash:private-config.text
Enable Break:       no
Manual Boot:         no
HELPER path-list:
NVRAM/Config file
    buffer size:     32768
```

Step 5

If there is no software image defined in the BOOT path-list, enter **dir flash:** to display the contents of Flash memory.

Step 6

Using the exact, case-sensitive name of the .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with .bin. The image filename is then the same as the downloaded filename but with a .bin extension. This step does not affect the operation of the switch.



Note

Perform this step only if you have space available on your switch and want to retain a copy of the old image.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename flash:c2950-i6q412-mz.121-9.EA1.bin flash:c2950-i6q412-mz.121-11.EA1.bin
```

Step 7 Display the contents of Flash memory to verify the renaming of the file:

```
switch# dir flash:

Directory of flash:/
 3  drwx      10176   Mar 01 2001 00:04:34  html
 6  -rwx       2343   Mar 01 2001 03:18:16  config.text
171 -rwx      1667997   Mar 01 2001 00:02:39  c2950-i6q412-mz.121-11.EA1.bin
 7  -rwx       3060   Mar 01 2001 00:14:20  vlan.dat
172 -rwx         100   Mar 01 2001 00:02:54  env_vars
```

7741440 bytes total (4788224 bytes free)

Step 8 Enter global configuration mode:

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

Step 9 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.121-11.EA1.bin
```



Note

If the **show boot** command entered in [Step 4](#) 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 10 Return to privileged EXEC mode:

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

Step 11 Remove the HTML files:

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

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

Step 12 Start the TFTP copy function as if you were initiating it from the command switch.



Caution

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

```
switch-1# archive tar /x tftp://server_ip_address/path/filename.tar flash:
Source IP address or hostname [server_ip_address]?
Source filename [path/filename]?
Destination filename [flash:new_image]?
Loading /path/filename.bin from server_ip_address (via!)
[OK - 843975 bytes]
```

Step 13 Enter global configuration mode:

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

Step 14 Return to privileged EXEC mode:

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

Step 15 Reload the new software with this command:

```
switch-1# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

Press **Enter** to start the download.

You lose contact with the switch while it reloads the software. For more information on the **rcommand** command, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

Upgrading Catalyst 1900 or Catalyst 2820 Member Switches

Follow these steps to upgrade the software on a Catalyst 1900 or Catalyst 2820 member switch:

Step 1 In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, select the number of the member switch that you want to upgrade. The member number is in the SN column of the display. You need this member number for Step 2.

Step 2 Log in to the member switch (for example, member number 1):

```
switch# rcommand 1
```

Step 3 For switches running the standard edition software, enter the password (if prompted), access the Firmware Configuration menu from the menu console, and perform the upgrade. Follow the instructions in the installation and configuration guide that shipped with your switch. When the download is complete, the switch resets and begins using the new software.

The Telnet session accesses the menu console (the menu-driven interface) if the command switch password is privilege level 15. If the command switch password is privilege level 1, you are prompted for the password.

You lose contact with the switch while it reloads the software.

Step 4 For switches running Enterprise Edition Software, start the TFTP copy as if you were initiating it from the member switch:

```
switch-1# copy tftp://host/src_file opcode
```

For example, **copy tftp://spaniel/op.bin opcode** downloads new system operational code *op.bin* from the host *spaniel*.

You should see the `TFTP successfully downloaded operational code` message. When the download is complete, the switch resets and begins using the new software. If this message does not appear, refer to the installation and configuration guide that shipped with your switch for more information.

You can also upgrade the switch software through the Firmware Configuration menu from the menu console. For more information, refer to the installation and configuration guide that shipped with your switch.

You lose contact with the switch while it reloads the software.

Recovering from Software Failure

If the software fails, you can reload the software. For detailed recovery procedures, refer to the “Troubleshooting” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Installation Notes

You can assign IP information to your switch by using the setup program, the Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration (refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*), or by manually assigning an IP address (refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*).

This section describes these installation procedures:

- [“Setting Up the Catalyst 2950 Initial Configuration” section on page 18](#)
- [“Accessing CMS” section on page 20](#)

Setting Up the Catalyst 2950 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:

- Command-line interface (CLI)
- CMS from your browser

Accessing CMS

Before the browser can use the CMS, a Java plug-in is required, as described in the [“Installing the Required Plug-In” section on page 5](#). After you have assigned an IP address to the switch and installed the plug-in, you can access the switch from your browser and use the CMS to configure other switches.

**Note**

If you have downloaded a new version of the CMS, you must clear your browser cache before launching the new CMS version.

To use the web-based tools, see the [“Software Compatibility” section on page 3](#) to set up the appropriate browser options.

To display the CMS access page, follow these steps:

Step 1 Enter the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), and press **Return**.

Step 2 Enter your username and password when prompted.



Note The browser always prompts for username and password. If no username is configured on your switch, you only need to enter the enable password in the appropriate field.

The Cisco Systems Access page appears. For more information on setting passwords and privilege levels, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Step 3 Click **Web Console** to launch the CMS applet.

When you access CMS from a standalone or a cluster-member switch, Device Manager appears.

New Software Features

There are no new software features in this release. For more information, refer to the *Release Notes for the Catalyst 2950 Desktop Switch, Release 12.1(11)EA1*.

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.

These are the limitations and restrictions:

- [“Immediate-Leave Limitation” section on page 21](#)
- [“RSPAN Limitation” section on page 22](#)
- [“Guidelines for Applying ACLs” section on page 22](#)
- [“Hardware and Software Compatibility Matrixes” section on page 22](#)
- [“Port Configuration Conflicts” section on page 24](#)
- [“SPAN Limitation” section on page 25](#)

Immediate-Leave Limitation

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)

RSPAN Limitation

In a Remote Switched Port Analyzer (RSPAN) session, if at least one Catalyst 2950 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.

Guidelines for Applying ACLs

Follow these guidelines for applying access control lists (ACLs) to interfaces:

- When you apply an ACL to a physical interface, some keywords are not supported, and certain mask restrictions apply to the ACLs. For information on creating ACLs for physical interfaces, refer to the “Creating a Numbered Standard ACL” section and the “Creating a Numbered Extended ACL” section of the software configuration guide for Release 12.1(11)EA1. (CSCdw56650)
- 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* and the *Command Reference for IOS Release 12.1*.

Hardware and Software Compatibility Matrixes

Some switches are not supported by certain software releases. In [Table 7](#) and [Table 8](#), *Yes* means that the switch is supported by the software release; *No* means that the switch is not supported by the release.

[Table 7](#) 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.

[Table 8](#) lists the Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, 2950G-48-EI, and 2950SX-24 switches and the software releases supporting them. The serial numbers are on the switch rear panel.

Table 7 Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches

Hardware	Serial Number	Release 12.0(5)WC2b or Earlier	Release 12.1(6)EA2, Release 12.1(6)EA2a, and Release 12.1(6)EA2b	Release 12.1(6)EA2c	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 7 Catalyst 2950-12, 2950-24, 2950C-24, and 2950T-24 Switches (continued)

Hardware	Serial Number	Release 12.0(5)WC2b or Earlier	Release 12.1(6)EA2, Release 12.1(6)EA2a, and Release 12.1(6)EA2b	Release 12.1(6)EA2c	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

Table 8 Catalyst 2950G-12-EI, 2950G-24-EI, 2950G-24-EI-DC, 2950G-48-EI, and 2950SX-24 Switches

Hardware	Release 12.0(5)WC2b or Earlier	Release 12.1(6)EA2, Release 12.1(6)EA2a, and Release 12.1(6)EA2b	Release 12.1(6)EA2c	Release 12.1(9)EA1	Release 12.1(9)EA1d or Later
Catalyst 2950G-12-EI	No	Yes	Yes	Yes	Yes
Catalyst 2950G-24-EI	No	Yes	Yes	Yes	Yes
Catalyst 2950G-24-EI-DC	No	Yes	Yes	Yes	Yes
Catalyst 2950G-48-EI	No	Yes	Yes	Yes	Yes
Catalyst 2950SX-24	No	No	No	No	Yes

Port Configuration Conflicts

Certain combinations of port features create configuration conflicts (see [Table 9](#)). If you try to enable incompatible features, CMS issues a warning message, and you cannot make the change. Reload the page to refresh CMS.

In [Table 9](#), *No* means that the two referenced features are incompatible, and both should not be enabled; *Yes* means that both can be enabled at the same time and do not cause an incompatibility conflict. A dash means not applicable.

Table 9 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	No
SPAN Source Port	Yes	Yes	–	No	Yes	Yes ¹	Yes

Table 9 *Conflicting Features (continued)*

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

1. Switched Port Analyzer (SPAN) cannot operate if the monitor port or the port being monitored is not a protected port.

SPAN Limitation

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.

Important Notes

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

- [“CMS Notes” section on page 25](#)
- [“Changing the Management VLAN” section on page 26](#)
- [“IGMP Filtering” section on page 26](#)

CMS Notes

This section describe this information:

- [Read-Only Mode in CMS, page 25](#)
- [Configuring CMS, page 26](#)

Read-Only Mode in CMS

CMS provides two levels of access to the configuration options. If your privilege level is 15, you have read-write access to CMS. If your switch privilege level is from 1 to 14, you have read-only access to CMS. In the read-only mode, some data is not displayed, and an error message appears when these switches are running these software releases:

- Catalyst 2900 XL or Catalyst 3500 XL member switches running Release 12.0(5)WC2 or earlier
- Catalyst 2950 member switches running Release 12.0(5)WC2 or earlier
- Catalyst 3550 member switches running Release 12.1(6)EA1 or earlier

In the Front Panel view or Topology view, CMS does not display error messages. 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 a Long-Reach Ethernet (LRE) switch, the customer premises equipment (CPEs) connected to the switch do not appear. The Bandwidth and Link graphs also do not appear in these views.

To view switch information, you need to upgrade the member switch software. For information about upgrading switch software, see the [“Downloading Software” section on page 7](#).

Configuring CMS

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 use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.add.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.
- If you use the Netscape browser to view the CMS GUI and you resize the browser window while CMS is initializing, CMS does not resize to fit the window.

Resize the browser window again when CMS is not busy.

- CMS does not start if the temporary directory on your computer runs out of memory. This problem can occur because of a bug in the 1.2.2 version of the Java plug-in. The plug-in creates temporary files in the directory whenever it runs CMS, and the directory eventually runs out of plug-in space.

The workaround is to remove all the *jar_cache*.tmp* files from the temporary directory. The path to the directory is different for different operating systems:

```
Solaris: /var/tmp
Windows NT and Windows 2000: \TEMP
Windows 95 and 98: \Windows\Temp
```

Changing the Management VLAN

The **management** interface configuration command is not supported in 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 Desktop Switch Command Reference* for information about using the **shutdown** interface configuration command.

IGMP Filtering

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

Open Caveats

These are the open caveats in this release:

- [“Open IOS Caveats” section on page 27](#)
- [“Open Cluster Configuration Caveats” section on page 32](#)
- [“Open CMS Caveats” section on page 33](#)

Open IOS Caveats

These are the severity 3 IOS configuration caveats:

- CSCdv82224

If a stack that has Catalyst 2950 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.

- CSCdw48441

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 Release 12.1(6)EA2 or earlier.

There is no workaround.

- CSCdx65965

When a switch is first turned on, it can obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server. After the switch is restarted with the service configuration option, it can no longer obtain an IP address from a DHCP server.

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

- CSCdx75308

When you use the **policy-map** global configuration command to create a policy map, and you do not specify any action for a classmap, 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.

- CSCdx93122

On a Catalyst 2950 switch that is running Release 12.1(9)EA1 or earlier, the default VLANs cannot be removed from the allowed list on a trunk port, and only one management VLAN can be active at a time.



Note Any VLAN can be removed except for the default VLANs 1002 to 1005.

The workaround is to have only one active management VLAN at a time.

- CSCdy08716

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.

- CSCdx79221

When you set the `c2900PortUseageApplication` object value in the CISCO-C2900 MIB, to **monitor**, **portgroupDest**, **portGrouping**, **network**, or **networkGroup**, the setting is rejected.

The workaround for the **monitor** keyword is to use the CLI to configure a SPAN session.

The workaround for the **portGroupDest** and **portGrouping** values is to use the EtherChannel CLI commands to configure load balancing.

There are no workarounds for the **network** and **networkGroup** values. These are unsupported values.

- CSCdw02638

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.

- CSCdt27223

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.

- CSCdw06074

Layer 3 CPU packets from a SPAN-source port configured to monitor sent traffic are not mirrored to the SPAN-destination port on a Catalyst 2950 switch.

There is no workaround.

- CSCdv82224

If a stack contains Catalyst 3550, 3500 XL, or 2900 XL switches, then the CSUF feature does not work if the management VLAN on these switches is changed to a VLAN other than VLAN 1.

The workaround is to ensure that the management VLAN of all the Catalyst 3550, 3500 XL, and 2900 XL switches in the stack is set to VLAN 1.

- CSCdv02941

In some network topologies, when UplinkFast is enabled on all Catalyst 2950 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.
- CSCdv19671

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 userid that causes the 802.1X port to be deauthenticated.

The workaround is to manually re-initiate authentication by either logging off or detaching the link and then re-connecting it.
- CSCdv67047

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.
- CSCdv44005

A Catalyst 2950 command switch running Release 12.1(6)EA2 cannot use the **rcommand** privileged EXEC command to start a Telnet session on a Catalyst 3550 member running IOS Release 12.1(4)EA1, when the **aaa authorization exec default group tacacs+** global configuration command is configured on both the command switch and the member.

The workaround is to upgrade the Catalyst 3550 switch to Release 12.1(6)EA1a.
- CSCdv34505

The Catalyst 2950 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.
- CSCdv62271

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 auto-negotiation.
- CSCdu83640

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.

- CSCdv49871

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.

- CSCdv27247

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.

- CSCdv45190

On a Catalyst 2950 switch, the Multicast VLAN Registration (MVR) receiver port joins only 255 groups when the Internet Group Management Protocol (IGMP) join message is sent to all 256 MVR groups configured. Multicast data for the 256th group is not received.

The workaround is to set the mode to **dynamic** for Catalyst 2950 switches that are connected to IGMP-capable devices. Then, MVR members can join any group but can only support 255 IP multicast streams at any given time.

- CSCdt24814 (formerly CSCdt2481)

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.

- CSCdt48011

Two problems occur when the Catalyst 2950 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.

- CSCds20365

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.

- CSCdt83016

When the Catalyst 2950 switch boots up without being configured, it prompts the user with a configuration dialog. The switch allows the user to omit the dialog and to enable traps without configuring a community string. If the host trap receiver is configured without defining the community strings, when the switch attempts to generate a trap, it fails and displays an error message.

The workaround is to follow the configuration sequence by creating a community string before configuring traps for the host.
- CSCdr96565

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.
- CSCdt48569

If any VLAN other than VLAN 1 is configured as the management VLAN, the switch reports an incorrect shutdown for VLAN 1. VLAN 1 is not administratively down, even though the running configuration has shut down in VLAN 1.

There is no workaround.
- CSCds68177

The UniDirectional Link Detection (UDLD) protocol does not always detect a unidirectional link when there is a loop between the TX and RX strands on the same port (TX/RX loop condition).

This is an intermittent problem, and there is no workaround.
- CSCds58369

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.
- CSCdp70389

When changing the management VLAN on a cluster with command-switch redundancy enabled, the cluster can break if Hot Standby Router Protocol (HSRP) is configured on any of the cluster members in the new management VLAN.

The workaround is to not change the management VLAN to a VLAN where a member is configured as part of a standby group.
- CSCdp85954

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.
- CSCdp49419

HSRP does not support a virtual MAC address entry or a built-in address (BIA) for a cluster.

There is no workaround.

- CSCdp97517
All members of an HSRP standby group must be cluster members.
There is no workaround.
- CSCdp30543
If the storm control filter is enabled for unicast or multicast traffic and the rising threshold is reached, all traffic on the port is filtered. No unicast, multicast, or broadcast traffic is forwarded from the port.
There is no workaround.
- CSCdp87748
Cisco IOS does perform some checks on entered IP addresses. For example, it does not allow the broadcast address to be entered. However, it does not check for the broadcast address on the same subnet as the HSRP Versatile Interface Processor (VIP) or the management VLAN IP address. This means that you could configure HSRP with a virtual IP address that is the same as the network broadcast address.
There is no workaround.

Open Cluster Configuration Caveats


These are the severity 3 cluster caveats in this release:

- CSCdw10837
When a Catalyst 2950 cluster command switch is running Release 12.1(6)EA2 or later and you enter the **no cluster commander-address** global configuration command on a member switch of this cluster, the member switch cannot be removed from the cluster if there are any member switches beyond that member switch.
The workaround is to enter the **no cluster member n** global configuration command on the command switch to remove the member from the cluster.
- CSCdw01109
When a Catalyst 2950 switch is the cluster command switch of a Catalyst 3550 member switch, the Catalyst 3550 switch does not show any egress policy information in the Attach tab of the QoS Policies window.
There is no workaround.
- CSCdt09918
When the cluster command switch is a:
 - Catalyst 2900 XL switch
 - Catalyst 2950 switch running software earlier than Release 12.1(6)EA2
 - Catalyst 3500 XL switch that is connected to either a Catalyst 2950 switch running Release 12.1(6)EA2 or later or a Catalyst 3550 switch
 The command switch then does not find any cluster candidates beyond the Catalyst 2950 or 3550 switch if it is not a member of the cluster.
The workaround is to add the Catalyst 2950 or 3550 switch to the cluster. You can then see any cluster candidates connected to it.

- CSCdp82354
You can use Cluster Manager to configure a HSRP standby group and bind it to a cluster. However, you cannot use Cluster Manager to configure more than one standby group. If you want to configure more than one standby group, use the CLI.
There is no workaround.

Open CMS Caveats

These are the severity 3 CMS configuration caveats:

- CSCdw87550
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.
 **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.
- CSCdx88994
In read-only mode, time ranges are not displayed. See the [“CMS Notes” section on page 25](#) for more information about CMS modes.
There is no workaround.
- CSCdy17589
If you try to create a *time-range* entry that specifies multiple days with the same time, the CMS displays only the first day in the list of days. This is an example of such a time-range entry:

```
periodic Monday Wednesday Friday 8:00 to 17:00.
```


The periodic time-range entries with specific days use this syntax:

```
periodic Monday 8:00 to Tuesday 17:00.
```


or

```
periodic Monday 8:00 to Monday 17:00
```


The workaround is to create a specific time-range entry for each day.
- CSCdx76634
The data that is displayed by using the Stack Bar and Stack Area options in the Link Graph window is incorrect.
The workaround is to use the Line, Bar, or Area options instead.
- CSCdy36743
You cannot add a switch that does not have Terminal Access Control Access System Plus (TACACS+) configured on it to a cluster if all the other cluster members are configured with TACACS+.
The workaround is to configure TACACS+ on the switch before adding it to the cluster.
- CSCdv82352

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.



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

- CSCdy37017

When there are no CMS windows open, the CMS keyboard shortcuts do not work.

The workaround is to leave one CMS window open. For example, leave the **Help > About** window open.

- CSCdy30410

When a Catalyst 2950 switch becomes a command switch, it automatically creates an IP extended ACL called *CMP-NAT-ACL* that specifies a set of IP addresses subject to cluster-NAT address translation. Although CMS allows you to modify or delete this ACL, do not modify or delete this ACL.

There is no workaround.

- CSCdx94729

The cursor is not displayed in the text-entering areas in CMS. However, in some cases you can still enter text. This problem occurs with certain combinations of both the browser and the Java plug-in. For example, it can occur when Netscape Communicator 6.2.3 is used with Java Plug-In 1.3.1_02 or 1.3.1_03.

These are the two workarounds:

- Use a supported browser and Java plug-in. For more information, see [Table 4 on page 4](#).
- Click in a text-entering area outside CMS, such as in the browser. Make sure that the cursor appears, and then click in the text-entering area in CMS. The cursor should now appear. If it does not, restart CMS by clicking on the reload/refresh button or by restarting the browser.

- CSCdy47214

You cannot add a class to a new policy when you launch **Device > QoS > Policies** in Guide Mode. The workaround is to launch **Device > QoS > Policies** in Expert Mode, and then add the class to the policy.

- CSCdp67822

CMS requires a Java plug-in from Sun Microsystems. If you are using Internet Explorer and you disable Java plug-ins by using the Java Plug-In Control Panel, the initial Splash screen shows that the plug-in and Java are enabled, but Internet Explorer fails.

The workaround is to not disable Java plug-ins on the Java Plug-In Control Panel.

- CSCdp82224

The CMS Time Management window supports the configuration of the Network Time Protocol (NTP) and system time. When you make changes on this window from a command switch, Java propagates the changes to all cluster members. A conflict can arise if you configure NTP and also use the Set Daylight Saving Time and Set Current Time tabs.

To avoid a possible conflict, either set the system time for the entire cluster on the command switch, or configure NTP on the command switch to use an NTP server to provide time to the cluster. Do not use both methods at the same time.

- CSCdp75220

If you use the command switch Domain Name System (DNS) server name to start CMS for a member that is running an earlier software release than the command switch, CMS might not display the switch image, or it might display the command switch image. This can also occur when a standby group is configured for a cluster and you access CMS by entering the command-switch IP address and not the virtual IP address.

The workaround is to always use the command-switch IP address to access CMS. If a standby group is configured for a cluster, always use the virtual IP address to access CMS.

- CSCdp62807

If you click the list of switches in CMS and press the Page Down key on the keyboard, the entire list moves to the bottom of the window. This only happens with Windows NT.

The workaround is to collapse the list into a single icon, which returns the list to the top of the window.

- CSCdv56582

In the CMS topology view, icons for the fiber-optic, ATM, and FDDI links are not visible.

There is no workaround.

Resolved Caveats

These caveats were resolved in these releases:

- [“IOS Caveats Resolved in Release 12.1\(11\)EA1a” section on page 35](#)
- [“IOS Caveats Resolved in Release 12.1\(11\)EA1” section on page 36](#)

IOS Caveats Resolved in Release 12.1(11)EA1a

These IOS caveats were resolved in Release 12.1(11)EA1a:

- CSCdy11990

A switch no longer forwards unknown unicast and broadcast traffic from VLAN1 to dynamic access ports.

- CSCdy29736

Clients connected to dynamic switchports no longer intermittently send and receive data.

- CSCdy43265

When the spanning tree state changes from learning to forwarding or from forwarding to blocking, a switch now sends a topology change trap.

- CSCdy55350

A switch no longer reloads when the autoconfiguration file includes VLAN configuration settings.

- CSCdy58823

The UniDirectional Link Detection (UDLD) protocol no longer disables Gigabit ports during startup when a mismatch state occurs with neighboring switches.

- CSCdy708510
If you enter the **switchport port-security mac-address sticky** and **switchport port-security violation shutdown** interface configuration commands on an interface, when a security violation occurs, the interface is errdisabled.
- CSCdy71638
A switch no longer removes dynamic MAC addresses from the MAC address table before the specified aging time.

IOS Caveats Resolved in Release 12.1(11)EA1

These IOS caveats were resolved in Release 12.1(11)EA1:

- CSCuk33625
In MVR mode, when multicast data is received on a port that is in STP blocked state, the switch no longer loses bridge protocol data unit (BPDU) packets, and STP loops are no longer created.
- CSCdx67634
The default encapsulation is changed from dot1q to native for a SPAN destination port. You can now configure dot1q encapsulation for a SPAN destination port.
- CSCdx33135
When sticky learning is enabled, addresses that are dynamically learned on a secure port are retained by the switch after it reboots.
- CSCdy11748
You can disable autonegotiation on 1000BASE-SX, -LX, and -ZX Gigabit Interface Converter (GBIC) ports by using the **speed nonegotiate** interface command.



Note Gigastack GBICs and 1000BASE-T GBICs do not support the **speed nonegotiate** interface command.

- CSCdx87698
When an access control list (ACL) that has no access control entry (ACE) is applied to a class map, you can now remove the ACL from the class map by using the **no match access-group** class-map configuration command.
- CSCdx29415
In an UplinkFast network topology, the alternate port becomes the root port when the original root port loses connectivity. On switches running Release 12.1(6)EA2 or later, if connectivity is restored on the original root port, dummy multicast frames are now sent from that port.
- CSCdw59136
When a switch is in VTP transparent mode, and it receives frames from a trunk port with an unknown VLAN ID number, certain frames are no longer sent to the same trunk port with a VLAN ID that is the same as the switch management VLAN and a source MAC address that is the same as its destination MAC address.
- CSCdw06738
A traffic interruption no longer occurs for several seconds during a cross-stack UplinkFast (CSUF) root-port transition.

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>

This section provides updates to the product documentation.

These changes will be included in the next version of the documentation.

Addition to the Catalyst 2950 Software Configuration Guide (CSCdy70850)

This information about secure MAC addresses was added for this release:

- The switch does not support port security aging of sticky secure MAC addresses.
- When sticky secure addresses are dynamically learned, if a security violation occurs, the violation mode (protect, restrict, or shutdown) takes affect.
- When you specify sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, if a security violation occurs, the violation mode does not take affect.
- When you specify static secure MAC addresses by using the **switchport port-security mac-address** *mac-address* interface configuration command, if a security violation occurs, the violation mode does not take affect.

If a security violation occurs, you can configure the interface for one of three violation modes, based on the action to be taken:

- **protect**—When the number of secure MAC addresses reaches the maximum allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict**—A port security violation restricts data from unknown source addresses.
- **shutdown**—When a port security violation occurs, the interface is error-disabled and the port LED is off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** *psecure-violation* global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands. This violation mode is the default mode.

When a security violation occurs, an SNMP a syslog message might be sent, an error message might appear, or the SecurityViolation counter in the **show ports-security** privileged EXEC command out put might increment. [Table 10](#) lists the actions that occur when these MAC address are configured on the interface:

- static secure MAC addresses
- dynamic secure MAC addresses
- sticky secure addresses that are manually configured
- sticky secure addresses that are dynamically learned

In [Table 10](#), *Yes* means that the action occurs. *No* means that the action does not occur.

Table 10 Actions When Security Violations Occur

Secure MAC Address Type	Violation Mode	Traffic is forwarded	SNMP trap is sent ¹	Syslog message is sent	CLI error message appears	SecurityViolation counter increments
Secure MAC addresses that are manually configured	protect	No	No	No	Yes	No
	restrict	No	No	No	Yes	No
	shutdown	No	No	No	Yes	No
Secure MAC addresses that are dynamically learned	protect	No	No	No	No	No
	restrict	No	Yes	Yes	No	Yes
	shutdown	No	Yes	Yes	No	Yes

1. SNMP traps are only supported on the Catalyst 2950 switches.

For more information about secure MAC addresses, refer to the “Secure MAC Addresses” section in the “Configuring Port-Based Traffic Control” chapter in the software configuration guide for this release.

For more information about security violations, refer to the “Security Violations” section in the “Configuring Port-Based Traffic Control” chapter in the software configuration guide for this release.

Addition to the Command Reference (CSCdy70850)

The **clear port-security sticky** privileged EXEC command was added for this release.

clear port-security sticky

Use the **clear port-security sticky** privileged EXEC command to delete from the secure MAC address table a specific sticky secure address, all the sticky secure addresses on an interface, or all the sticky secure addresses on the switch.

clear port-security sticky [**address** *mac-addr* | **interface** *interface-id*]

Syntax Description	
address <i>mac-addr</i>	(Optional) Delete the specified sticky secure MAC address.
interface <i>interface-id</i>	(Optional) Delete all the sticky secure MAC addresses on the specified physical port.

Defaults No default is defined.

Command Modes Privileged EXEC

Usage Guidelines

If you enter the **clear port-security sticky** privileged EXEC command without keywords, the switch removes all sticky secure MAC addresses from the secure MAC address table.

If you enter the **clear port-security sticky address** *mac-addr* command, the switch removes the specified secure MAC address from the secure MAC address table.

If you enter the **clear port-security sticky interface** *interface-id* command, the switch removes all sticky secure MAC addresses on an interface from the secure MAC address table.

Command History

Release	Modification
12.1(11)EA1a	This command was first introduced.

Examples

This example shows how to remove a specific sticky secure address from the secure MAC address table:

```
Switch# clear port-security sticky address 0008.0070.0007
```

This example shows how to remove all the sticky secure addresses learned on a specific interface:

```
Switch# clear port-security sticky interface gigabitethernet0/1
```

This example shows how to remove all the sticky secure addresses from the secure MAC address table:

```
Switch# clear port-security sticky
```

You can verify that the information was deleted by entering the **show port-security** address privileged EXEC command.

Related Commands

Command	Description
switch port-security	Enables port security on an interface.
switchport port-security mac-address sticky	Enables the interface for sticky learning.
switchport port-security mac-address sticky <i>mac-address</i>	Specifies a sticky secure MAC address
switchport port-security maximum <i>value</i>	Configures a maximum number of secure MAC addresses on a secure interface.
show port-security address	Displays the port security settings defined for an interface or for the switch.

Addition to the Command Reference

The **ip igmp snooping source-only-learning** global configuration command was omitted in the *Catalyst 2950 Desktop Switch Command Reference* for this release.

ip igmp snooping source-only-learning

Use the **ip igmp snooping source-only-learning** global configuration command to enable IP multicast-source-only learning on the switch. Use the **no** form of this command to disable IP multicast-source-only learning.

ip igmp snooping source-only-learning

no ip igmp snooping source-only-learning

Syntax Description

This command has no arguments or keywords.

Defaults

IP multicast-source-only learning is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11)EA1	This command was first introduced.

Usage Guidelines

When IP multicast-source-only learning is enabled, the switch learns the IP multicast group from the IP multicast data stream and only forwards traffic to the multicast router ports.



Note

We strongly recommend that you do not disable IP multicast-source-only learning. IP multicast-source-only learning should be disabled only if your network is not composed of IP multicast-source-only networks and if disabling this learning method improves the network performance.

Examples

This example shows how to disable source-only learning:

```
Switch(config)# no ip igmp snooping source-only-learning
```

This example shows how to enable source-only learning:

```
Switch(config)# ip igmp snooping source-only-learning
```

You can verify your settings by entering the **show running-config | include source-only-learning** privileged EXEC command.

Related Commands	Command	Description
	ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
	show running-config include source-only-learning	Displays the configuration information running on the switch. For syntax information, select Cisco IOS Configuration Fundamentals Command Reference for Release 12.1 > Cisco IOS File Management Commands > Configuration File Commands .

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 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 41.

These publications provide more information about the switches:

- *Catalyst 2950 Desktop Switch Software Configuration Guide* (order number DOC-7811380=)
- *Catalyst 2950 Desktop Switch Command Reference* (order number DOC-7811381=)
- *Catalyst 2950 Desktop Switch System Message Guide* (order number DOC-7814233=)
- *Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (DOC-786460=)
- Cluster Management Suite (CMS) online help
- *CWDM Passive Optical System Installation Note* (not orderable but is available on Cisco.com)
- *1000BASE-T Gigabit Interface Converter Installation Notes* (not orderable but is available on Cisco.com)

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

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 is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

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/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- 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. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Website

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, 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 Web Site. The Cisco TAC Web Site requires 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://www.cisco.com/register/>

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

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 level of 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.

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

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0208R)

Copyright ©2001-2002, Cisco Systems, Inc.
All rights reserved.