



# Release Notes for the Catalyst 2960 Switches, Cisco IOS Release 12.2(25)FX

---

**November 4, 2005**

The Cisco IOS Release 12.2(25)FX runs on all Catalyst 2960 switches.

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

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 5.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Deciding Which Files to Use](#)” section on page 5.

For the complete list of Catalyst 2960 switch documentation, see the “[Related Documentation](#)” section on page 14.

You can download the switch software from this site (registered Cisco.com users with a login password):  
<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Cisco IOS Release 12.2(25)FX is based on Cisco IOS Release 12.2(25)SEB4. Open caveats in Cisco IOS Release 12.2(25)SEB4 also affect Cisco IOS Release 12.2(25)FX, unless they are listed in the Cisco IOS Release 12.2(25)FX resolved caveats list. The list of open caveats in Cisco IOS Release 12.2(25)SEB4 is available at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225seb/ol7189.htm>



---

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

© 2005 Cisco Systems, Inc. All rights reserved.

# Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Upgrading the Switch Software” section on page 5](#)
- [“Installation Notes” section on page 8](#)
- [“New Features” section on page 8](#)
- [“Limitations and Restrictions” section on page 8](#)
- [“Important Notes” section on page 12](#)
- [“Resolved Caveats” section on page 14](#)
- [“Related Documentation” section on page 14](#)
- [“Obtaining Documentation” section on page 15](#)
- [“Documentation Feedback” section on page 16](#)
- [“Obtaining Technical Assistance” section on page 18](#)
- [“Obtaining Additional Publications and Information” section on page 19](#)

## System Requirements

The system requirements are described in these sections:

- [“Hardware Supported” section on page 3](#)
- [“Device Manager System Requirements” section on page 4](#)
- [“Cluster Compatibility” section on page 4](#)

## Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(25)FX.

**Table 1** Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960-24TC	24 10/100BASE-T Ethernet ports and 2 dual-purpose uplinks <sup>1</sup> (two 10/100/1000BASE-T copper ports and two SFP module slots)	Cisco IOS Release 12.2(25)FX
Catalyst 2960-48TC	48 10/100BASE-T Ethernet ports and 2 dual-purpose uplinks <sup>1</sup> (two 10/100/1000BASE-T copper ports and two SFP <sup>2</sup> module slots)	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24TT	24 10/100BASE-T Ethernet ports and 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-48TT	48 10/100BASE-T Ethernet ports 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-24TC	24 10/100/1000BASE-T Ethernet ports and 4 of these are dual-purpose uplinks <sup>1</sup> (four 10/100/1000BASE-T copper ports and four SFP module slots)	Cisco IOS Release 12.2(25)FX
SFP modules	1000BASE-BX, -CWDM <sup>3</sup> , -LX/LH, -SX, -ZX 100BASE-BX, FX, -LX	Cisco IOS Release 12.2(25)FX
Redundant power systems	Cisco RPS 300 Redundant Power System Cisco RPS 675 Redundant Power System	Supported on all software releases

1. Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.
2. SFP = small form-factor pluggable
3. CWDM = coarse wavelength-division multiplexer

## Device Manager System Requirements

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

- “[Hardware Requirements](#)” section on page 4
- “[Software Requirements](#)” section on page 4

### Hardware Requirements

[Table 2](#) lists the minimum hardware requirements for running the device manager.

**Table 2** Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II <sup>1</sup>	64 MB <sup>2</sup>	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

### Software Requirements

[Table 3](#) lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.



#### Note

The device manager does not require a plug-in.

**Table 3** Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer <sup>1</sup>	Netscape Navigator
Windows 98	None	5.5 or 6.0	7.1
Windows NT 4.0	Service Pack 6 or later	5.5 or 6.0	7.1
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

## Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch, unless your command switch is running Cisco IOS Release 12.1(19)EA1 or later.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 switches.

For additional information about clustering, see the “Clustering Switches” chapter of the software configuration guide.

## Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- [“Finding the Software Version and Feature Set” section on page 5](#)
- [“Deciding Which Files to Use” section on page 5](#)
- [“Upgrading a Switch by Using the Device Manager or Network Assistant” section on page 6](#)
- [“Archiving Software Images” section on page 6](#)
- [“Upgrading a Switch by Using the CLI” section on page 7](#)
- [“Recovering from a Software Failure” section on page 7](#)

## Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

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

## Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 4 lists the filenames for this software release.

**Table 4 Cisco IOS Software Image Files**

Filename	Description
c2960-lanbase-tar.122-25.FX.tar	Catalyst 2960 image file and device manager files. This image has Layer 2+ features.
c2960-lanbasek9-tar.122-25.FX.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.

## Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.



**Note**

When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

## Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/prod\\_bulletin0900aecd80281c0e.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html)

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.



**Note**

Although you can copy any file on the flash memory to the TFTP server, it is time-consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the “Basic File Transfer Services Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun\\_r/ffrprt2/frf011.htm#wp1018426](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt2/frf011.htm#wp1018426)

## Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

- 
- Step 1** Use [Table 4 on page 6](#) to identify the file that you want to download.
- Step 2** Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

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

To download the image for a Catalyst 2960 switch, click **Catalyst 2960 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2960 3DES Cryptographic Software**.

- Step 3** Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

- Step 4** Log into the switch through the console port or a Telnet session.

- Step 5** (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

- Step 6** Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
archive download-sw /overwrite /reload tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For *//location*, specify the IP address of the TFTP server.

For */directory/image-name.tar*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/c2960-lanbase-tar.122-25.FX.tar
```

You also can download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

## Recovering from a Software Failure

For recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

# Installation Notes

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

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

## New Features

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

- [“New Hardware Features” section on page 8](#)
- [“New Software Features” section on page 8](#)

## New Hardware Features

For a list of all supported hardware, see the [“Hardware Supported” section on page 3](#).

## New Software Features

This release is the first software release for the Catalyst 2960 switch. For a detailed list of key features for this software release, refer to the *Catalyst 2960 Switch Software Configuration Guide*.

## Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

- [“Cisco IOS Limitations” section on page 8](#)
- [“Device Manager Limitations and Restrictions” section on page 12](#)

## Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 2960 switches:

- [“Configuration” section on page 9](#)
- [“HSRP” section on page 9](#)
- [“IP” section on page 10](#)



- “IP Telephony” section on page 10
- “Multicasting” section on page 10
- “QoS” section on page 11
- “SPAN” section on page 11
- “Trunking” section on page 12
- “VLAN” section on page 12

## Configuration

These are the configuration limitations:

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

This problem occurs under these conditions:

- When the switch is booted without a configuration (no config.text file in flash memory).
- When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
- When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mbps full duplex or 100 Mbps half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

The workaround is to configure the port for 10 Mbps and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

## HSRP

This is the Hot Standby Routing Protocol (HSRP) limitation:

- When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list. The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

## IP

This is the IP limitation:

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

## IP Telephony

These are the IP telephony limitations:

- Some access point (AP)-350 devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These APs should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the AP-350 as an IEEE Class 1 device. The workaround is to power the AP by using an AC wall adaptor. (CSCin69533)
- When a Cisco IP Phone is connected to the switch, the port VLAN ID (PVID) and the voice VLAN ID (VVID) both learn its MAC address. However, after dynamic MAC addresses are deleted, only the VVID relearns the phone MAC address. MAC addresses are manually or automatically deleted when a topology change occurs or when port security or an 802.1x feature is enabled or disabled. There is no workaround. (CSCea80105)
- After you change the access VLAN on a port that has 802.1x enabled, the IP Phone address is removed. Because learning is restricted on 802.1x capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)

## Multicasting

These are the multicasting limitations:

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW\_NEW\_SOURCE record is before the BLOCK\_OLD\_SOURCE record, the switch removes the port from the group.
  - If the BLOCK\_OLD\_SOURCE record is before the ALLOW\_NEW\_SOURCE record, the switch adds the port to the group.

There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

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

There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

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

- When more multicast groups are configured for a port than are supported by the selected SDM template, traffic is flooded onto and dropped from the port.

There is no workaround. (CSCef67261)

## QoS

These are the quality of service (QoS) limitations:

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

## SPAN

This is the SPAN limitation:

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session session\_number destination {interface interface-id encapsulation replicate}** global configuration command for local SPAN. (CSCed24036)

## Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the LED to blink amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

## VLAN

This is the VLAN limitation:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.  
The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

## Device Manager Limitations and Restrictions

These are the device manager limitations and restrictions for this release:

- This release supports the same switch cluster compatibilities supported in Cisco IOS Release 12.1(22)EA1. However, you cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or the Cisco Network Assistant application. For information about Network Assistant, see the [“New Features” section on page 8](#).
- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.  
The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

## Important Notes

These sections describe the important notes related to this software release for the Catalyst 2960 switches:

- [“Cisco IOS Notes” section on page 13](#)
- [“Device Manager Notes” section on page 13](#)

## Cisco IOS Notes

There are no notes for Cisco IOS software in this release.

## Device Manager Notes

These notes apply to the device manager:

- We recommend this browser setting to speed up the time to display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

- Choose **Tools > Internet Options**.
  - Click **Settings** in the “Temporary Internet files” area.
  - From the Settings window, choose **Automatically**.
  - Click **OK**.
  - Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

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

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

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

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

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

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

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

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

## Resolved Caveats

These are the resolved caveats in this software release:

- CSCei61732

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

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

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

## Related Documentation

These documents provide complete information about the Catalyst 2960 switches and are available at Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2960/index.htm>

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “Obtaining Documentation” section on page 15.

These documents provide complete information about the Catalyst 2960 switches:

- *Catalyst 2960 Switch Software Configuration Guide* (order number DOC-7816881=)
- *Catalyst 2960 Switch Command Reference* (order number DOC-7816882=)
- *Catalyst 2960 Switch System Message Guide* (order number DOC-7816883=)
- Device manager online help (available on the switch)
- *Catalyst 2960 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide* (order number DOC-7816879=)
- *Regulatory Compliance and Safety Information for the Catalyst 2970 Switch* (order number DOC-7816880=)

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (not orderable but available on Cisco.com)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide* (order number DOC-7810372=)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)

## Obtaining Documentation

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

### Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

## Product Documentation DVD

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

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

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

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

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

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

## Documentation Feedback

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

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

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

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

We appreciate your comments.



# Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

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

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

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

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

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

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

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

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

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

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

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



**Tip**

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

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

# Obtaining Technical Assistance

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

## Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

## Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

## Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

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

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

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

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

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

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

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

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

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

---

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

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

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