



# Release Notes for the Catalyst 3750, 3560, and 2970 Switches, Cisco IOS Release 12.2(25)SE

---

**Revised April 2005**

The Cisco IOS Release 12.2(25)SE runs on all Catalyst 3750, 3560, and 2970 switches.

The Catalyst 3750 switches support stacking through Cisco StackWise technology. The Catalyst 3560 and 2970 switches do not support switch stacking. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.



**Note**

Beginning with this release, Cluster Management Suite (CMS) is no longer available with the switch software. You can use the embedded GUI (referred to as *device manager*) or the Network Assistant standalone application (available on Cisco.com) to manage one more switches. For more information about the device manager and the Network Assistant application, see the “[New Software Features](#)” [section on page 9](#).

---

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 6](#).

For the complete list of Catalyst 3750, 3560, and 2970 switch documentation, see the “[Related Documentation](#)” [section on page 34](#).

You can download the switch software from these sites:

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



---

**Corporate Headquarters:**

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

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 (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](#)
- [“Cluster Compatibility” section on page 4](#)
- [“Installation Notes” section on page 8](#)
- [“New Features” section on page 9](#)
- [“Minimum Cisco IOS Release for Major Features” section on page 10](#)
- [“Limitations and Restrictions” section on page 11](#)
- [“Important Notes” section on page 22](#)
- [“Open IOS Caveats” section on page 25](#)
- [“Resolved Caveats” section on page 29](#)
- [“Documentation Updates” section on page 32](#)
- [“Related Documentation” section on page 34](#)
- [“Obtaining Documentation” section on page 35](#)
- [“Documentation Feedback” section on page 36](#)
- [“Obtaining Technical Assistance” section on page 36](#)
- [“Obtaining Additional Publications and Information” section on page 38](#)

## 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 12.2SE.

**Table 1 Catalyst 3750, 3560, and 2970 Supported Hardware**

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750G-12S	12 SFP <sup>1</sup> module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-48TS	48 10/100 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-24PS	24 10/100 PoE <sup>2</sup> ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-16TD	16 10/100/1000 ports and 1 XENPAK 10-Gigabit Ethernet module port	Cisco IOS Release 12.2(18)SE
Catalyst 3560-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 2970G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 2970G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
SFP modules	1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, and CWDM <sup>3</sup>	Cisco IOS Release 12.2(18)SE
	100BASE-FX MMF <sup>4</sup>	Cisco IOS Release 12.2(20)SE
Redundant power systems	Cisco RPS 300 Redundant Power System (not supported on the Catalyst 3560 switch)	Supported on all software releases
	Cisco RPS 675 Redundant Power System	

1. SFP = small form-factor pluggable

2. PoE = Power over Ethernet

3. CWDM = coarse wavelength-division multiplexer

4. MMF = multimode fiber

## 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 *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, and the command reference.

## Upgrading the Switch Software

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 6](#)
- [“Upgrading a Switch by Using the Device Manager or Network Assistant” section on page 7](#)
- [“Upgrading a Switch by Using the CLI” section on page 7](#)
- [“Recovering from a Software Failure” section on page 8](#)

## 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.



### Note

For Catalyst 3750 and 3560 switches, although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (standard multilayer image [SMI] or enhanced multilayer image [EMI]) and does not change if you upgrade the software image.

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
c3750-i9-tar.122-25.SE.tar	Catalyst 3750 SMI file and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3750-i5-tar.122-25.SE.tar	Catalyst 3750 EMI file and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3750-i9k91-tar.122-25.SE.tar	Catalyst 3750 SMI cryptographic file and device manager files. This image has the Kerberos, SSH <sup>1</sup> , and Layer 2+, and basic Layer 3 routing features.
c3750-i5k91-tar.122-25.SE.tar	Catalyst 3750 EMI cryptographic file and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3560-i9-tar.122-25.SE.tar	Catalyst 3560 SMI file and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3560-i5-tar.122-25.SE.tar	Catalyst 3560 EMI file and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3560-i9k91-tar.122-25.SE.tar	Catalyst 3560 SMI cryptographic file and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3560-i5k91-tar.122-25.SE.tar	Catalyst 3560 EMI cryptographic file and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c2970-i6l2-tar.122-25.SE.tar	Catalyst 2970 image file and device manager files. This image has Layer 2+ features.
c2970-i6k9112-tar.122-25.SE.tar	Catalyst 2970 cryptographic image file and device manager files. This image has the Kerberos and SSH features.

1. SSH = Secure Shell

## 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.

## 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>

- If you do not have a SmartNet contract, go to this URL, and 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 image for a Catalyst 2970 switch, click **Catalyst 2970 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2970 3DES Cryptographic Software**.

To download the EMI or SMI files for a Catalyst 3560 switch, click **Catalyst 3560 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560 3DES Cryptographic Software**.

To download the EMI or SMI files for a Catalyst 3750 switch, click **Catalyst 3750 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750 3DES Cryptographic Software**.



### Caution

If you are upgrading a Catalyst 3750 or a Catalyst 2970 switch that is running a release earlier than Cisco IOS Release 12.1(19)EA1c, this release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade and occurs the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.

**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/c3750-i5-tar.122-20.SE.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. For information about this guide, see the [“Documentation Updates” section on page 32](#).
- 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.



### Note

If you are upgrading a Catalyst 3750 or a 2950 switch running Cisco IOS Release 12.1(11)AX, which uses the 802.1x feature, you must re-enable 802.1x after upgrading the software. For more information, see the [“Cisco IOS Notes” section on page 22](#).



**Note**

When upgrading or downgrading from Cisco IOS Release 12.2(18)SE, you might need to reconfigure the switch with the same password that you were using when running Release 12.2(18)SE. This problem only occurs when changing from Cisco IOS Release 12.2(18)SE to any other release. (CSCed88768)

## New Features

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

- “New Hardware Features” section on page 9
- “New Software Features” section on page 9

## New Hardware Features

For a list of all supported hardware, see the “Hardware Supported” section on page 3.

## New Software Features

This release contains these new Catalyst 3750, 3560, and 2970 switch features or enhancements (available in all software images):

- Beginning with this release, Cluster Management Suite (CMS) is no longer available with the switch software. You can use the embedded device manager to configure or manage a single switch. You can use the standalone Network Assistant application to configure or manage one or more switches:
  - The device manager is included in the switch image and provides simplified management for a single switch. Its features, such as Smartports and color-coded graphs, make it easier to configure and monitor the switch. No special installation is required. After the switch is configured through the Express Setup program or through the CLI-based setup program, the device manager is accessible through a Microsoft Internet Explorer or Netscape Navigator browser session. For more information, refer to the device manager online help. For information on how to display the device manager, refer to the switch getting started guide.
  - Network Assistant provides a comprehensive set of features for managing single and multiple devices, including switch clusters, through a GUI. This application must be downloaded from Cisco.com and be installed on your PC. You can learn more about Network Assistant at this URL:  
<http://www.cisco.com/go/NetworkAssistant>
- Secure Socket Layer (SSL) version 3.0 support for the HTTP1.1 server authentication, encryption, and message integrity, and HTTP client authentication to allow secure HTTP communications (only available in the cryptographic software image)
- Storm-control enhancements:
  - Specify the traffic rate in packets per second or in bits per second at which broadcast, multicast, or unicast packets are received.
  - Specify an action to take when a storm control occurs on a port.

- Support for DSCP transparency. If DSCP transparency is enabled, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.
- Support for VLAN-based QoS and hierarchical policy maps on switch virtual interfaces (SVIs).

This release contains these new features and enhancements for Catalyst 3750 and 3560 switches:

- IEEE 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers, and Layer 2 protocol tunneling to ensure that the customer's network has complete Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), and VLAN Trunking Protocol (VTP) information about all users.
  - Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels.
  - Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors.
- You can now configure private-VLAN ports on interfaces configured for dynamic ARP inspection (EMI only).
- IP source guard is now supported in private VLANs (EMI only).

This release contains these new Catalyst 3750 and 3560 PoE-capable switch features and enhancements (available in all software images):

- On PoE switches, the new Cisco intelligent power management feature enables the powered device and the switch to negotiate through CDP messages for an agreed power-consumption level. The negotiation allows a high-powered Cisco powered device, which consumes more than 7 W, to operate at its highest power mode.
- On PoE switches, you can limit the power allowed on a port or pre-allocate (reserve) power for a port before the switch discovers the powered device.

## Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release required to support the major features of the Catalyst 3750, 3560, and 2970 switches.

**Table 5** *Catalyst 3750, 3560, and 2970 Switch Features and the Minimum Cisco IOS Release Required*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Support for DSCP transparency	12.2(25)SE	3750, 3560, 2970
Support for VLAN-based QoS and hierarchical policy maps on SVIs	12.2(25)SE	3750, 3560, 2970
Support for Cisco Network Assistant	12.2(25)SE	3750, 3560, 2970
Device manager	12.2(25)SE	3750, 3560, 2970
802.1Q tunneling and Layer 2 protocol tunneling	12.2(25)SE	3750, 3560
Layer 2 point-to-point tunneling and Layer 2 point-to-point tunneling bypass	12.2(25)SE	3750, 3560

**Table 5** *Catalyst 3750, 3560, and 2970 Switch Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Support for SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE	3750, 3560, 2970
Support for configuring private-VLAN ports on interfaces that are configured for dynamic ARP inspection (EMI only)	12.2(25)SE	3750 and 3560
Support for IP source guard on private VLANs (EMI only)	12.2(25)SE	3750 and 3560
Cisco intelligent power management to limit the power allowed on a port, or pre-allocate (reserve) power for a port.	12.2(25)SE	3750 and 3560
802.1x accounting and MIBs (IEEE8021-PAE-MIB and CISCO-PAE-MIB)	12.2(20)SE	3750, 3560, 2970
Dynamic ARP inspection (EMI only)	12.2(20)SE	3750, 3560
Flex Links	12.2(20)SE	3750, 3560, 2970
HTTP software upgrade (device manager or Network Assistant only)	12.2(20)SE	3750, 3560, 2970
IP source guard (EMI only)	12.2(20)SE	3750, 3560
Private VLAN (EMI only)	12.2(20)SE	3750, 3560
SFP diagnostic management interface	12.2(20)SE	3750, 3560, 2970
Switch stack offline configuration	12.2(20)SE	3750
Stack-ring activity statistics	12.2(20)SE	3750
Smartports macros	12.2(18)SE	3750, 3560, 2970

## 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 12](#)
- [“Device Manager Limitations and Restrictions” section on page 22](#)

## Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3750, 3560, and 2970 switches:

- [“Configuration” section on page 12](#)
- [“Ethernet” section on page 14](#)
- [“Fallback Bridging” section on page 14](#)
- [“HSRP” section on page 14](#)
- [“IP” section on page 15](#)
- [“IP Telephony” section on page 15](#)
- [“MAC Addressing” section on page 15](#)
- [“Multicasting” section on page 16](#)
- [“QoS” section on page 17](#)
- [“Routing” section on page 17](#)
- [“SPAN and RSPAN” section on page 18](#)
- [“Stacking \(Catalyst 3750 switch stack only\)” section on page 20](#)
- [“Trunking” section on page 21](#)
- [“VLAN” section on page 21](#)

## 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)

- (Catalyst 3750 or 3560 switches) When the **show interface** privileged EXEC is entered on a port that is running 802.1Q, inconsistent statistics from ports running 802.1Q might be reported. The workaround is to upgrade to Cisco IOS Release 12.1(20)EA1. (CSCec35100)
- (Catalyst 3750 or 3560 switches) When you change a port from a nonrouted port to a routed port or the reverse, the applied auto-QoS setting is not changed or updated when you verify it by using the **show running interface** or **show mls qos interface** user EXEC commands. These are the workarounds:
  1. Disable auto-QoS on the interface.
  2. Change the routed port to a nonrouted port or the reverse.
  3. Re-enable auto-QoS on the interface. (CSCec44169)

- The DHCP snooping binding database is not written to flash or a remote file in any of these situations:
  - (Catalyst 3750 switch) When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and peer work correctly.
  - (Catalyst 3750, 3560, or 2970 switches) The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is removed manually from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - (Catalyst 3750, 3560, or 2970 switches) The URL for the configured DHCP snooping database was replaced because the original URL is not accessible. The new URL might not take effect after the timeout of the old URL.

No workaround is necessary; these are the designed behaviors. (CSCed50819)

- (Catalyst 3750 or 3560 switches) When dynamic ARP inspection is enabled on a switch or switch stack, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

However, when dynamic ARP inspection is not enabled and jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)

- 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)

- (Catalyst 3750 switches) Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails will be lost.

When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which the command was entered.

There is no workaround. (CSCed95822)

- 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)

## Ethernet

These are the Ethernet limitations:

- Subnetwork Access Protocol (SNAP) encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)
- Link connectivity might be lost between some older models of the Intel Pro1000 NIC and the 10/100/1000 switch port interfaces. The loss of connectivity occurs between the NIC card and these switch ports:
  - Ports 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, 24 of the Catalyst 3750G-24T and 3750G-24TS switches
  - Ports 3, 4, 7, 8, 11, 12, 15, 16, 19, 20 of the Catalyst 2970G-24T and 2970G-24TS switches

These are the workarounds:

- Contact the NIC vendor, and obtain the latest driver for the card.
- Configure the interface for 1000 Mbps instead of for 10/100 Mbps.
- Connect the NIC to an interface that is not listed here. (CSCea77032)

For more information, enter *CSCea77032* in the Bug Toolkit at this URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>

## Fallback Bridging

These are the fallback bridging limitations:

- (Catalyst 3750 or 3560 switches) If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group. The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)
- (Catalyst 3750 or 3560 switches) Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group. The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the **no switchport port-security** interface configuration command. (CSCdz80499)

## 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

These are the IP limitations:

- (Catalyst 3750 or 3560 switches) The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)
- 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)
- (Catalyst 3750 or 3560 PoE-capable switches) The switch uses the IEEE classification to learn the maximum power consumption of a powered device before powering it. The switch grants power only when the maximum wattage configured on the port is less than or equal to the IEEE class maximum. This ensures that the switch power budget is not oversubscribed. There is no such mechanism in Cisco prestandard powered devices.

The workaround for networks with pre-standard powered devices is to leave the maximum wattage set at the default value (15.4 W). You can also configure the maximum wattage for the port for no less than the value the powered device reports as the power consumption through CDP messages. For networks with IEEE Class 0, 3, or 4 devices, do not configure the maximum wattage for the port at less than the default 15.4 W (15,400 milliwatts). (CSCee80668)

## MAC Addressing

This is the MAC addressing limitation:

(Catalyst 3750 or 3560 switches) When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

## Multicasting

These are the multicasting limitations:

- (Catalyst 3750 or 3560 switches) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches) Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem for the non-RPF traffic occurs. (CSCdu25219)
- 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)
- (Catalyst 3750 or 3560 switches) When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)
- (Catalyst 3750 switch stack) If the stack master is power cycled immediately after the **ip mroute** global configuration command is entered, there is a slight chance that this configuration change might be lost after the stack master changes. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands. There is no workaround. (CSCea71255)
- (Catalyst 3750 switches) When IP Protocol-Independent Multicast (PIM) is enabled on a tunnel interface, the switch incorrectly displays the `Multicast is not supported on tunnel interfaces` error message. IP PIM is not supported on tunnel interfaces. There is no workaround. (CSCeb75366)
- 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)

## 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)

## Routing

These are the routing limitations:

- (Catalyst 3750 or 3560 switches) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches) A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)
- On a Catalyst 3750 switch stack with a large number of switched virtual interfaces (SVIs), routes, or both on a fully populated nine-member switch stack, this message might appear when you reload the switch stack or add a switch to the stack:

```
%SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
Pool: I/O Free: 77124 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

This error message means there is a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the **show cef line** user EXEC command and verifying that the line card states are `up` and `sync`. No workaround is required because the problem is self-correcting. (CSCea71611)

- (Catalyst 3750 switches) A spanning-tree loop might occur if all of these conditions are true:
  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

The workaround is to change any one of the listed conditions. (CSCed53633)

## SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the replicate option. For a remote SPAN session, there is no workaround.

This is a hardware limitation and only applies to these switches (CSCdy72835):

- 2970G-24T
- 2970G-24TS
- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD

- (Catalyst 3750 or 3560 switches) Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the encapsulation replicate option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround.

This is a hardware limitation and only applies to these switches (CSCdy81521):

- 2970G-24T
- 2970G-24TS
- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD

- During periods of very high traffic, when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session.

This is a hardware limitation and only applies to these switches (CSCea72326):

- 2970G-24T
- 2970G-24TS
- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- (Catalyst 3750 or 3560 switches) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: *Decreased egress SPAN rate*. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)
- On Catalyst 3750 switches running Cisco IOS Release 12.1(14)EA1 and later and on Catalyst 3560 switches running Cisco IOS release 12.1(19)EA1 or later, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)
- 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)

## Stacking (Catalyst 3750 switch stack only)

These are the Catalyst 3750 switch stack limitations:

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)
- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual boot is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots. There is no workaround. (CSCec36644)
- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mbps egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch (such as a Catalyst 3750-24TS or 3750-48TS switch) than if it is on a Gigabit Ethernet switch (such as a Catalyst 3750G-24T or 3750G-24TS switch). There is no workaround. (CSCed00328)
- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost. The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)
- When the **switchport** and **no switchport** interface configuration commands are entered more than 20,000 times on a port of a Catalyst 3750 switch, all available memory is used, and the switch halts. There is no workaround. (CSCed54150)
- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master switch-over occurs on one of the Catalyst 3750 default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master switch-over cannot complete.  
The workaround is to complete the MAC address update by entering the **clear arp** privileged EXEC command. (CSCed62409)
- When a Catalyst 3750 switch is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded. There is no workaround. (CSCed70894)
- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the SMI and the old stack master was running the EMI.

Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the EMI or the SMI:

- If the stack master is running the EMI, all stack members have private VLAN enabled.
- If the stack master is running SMI, all stack members have private VLAN disabled.

This occurs after a master-switchover (MSO) when the previous stack master was running the EMI and the new stack master is running the SMI. The stack members are configured with private VLAN, but any new switch that joins the stack will have private VLAN disabled.

These are the workarounds. Only one of these is necessary:

- Reload the stack after an EMI to SMI MSO (or the reverse).
- Before an EMI-to-SMI MSO, delete the private-VLAN configuration from the existing stack master. (CSCee06802)
- Port configuration information is lost when changing from **switchport** to **no switchport** modes on Catalyst 3750 switches.

This is the expected behavior of the offline configuration (provisioning) feature. There is no workaround. (CSCee12431)

## 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).
- If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch stack is on a different switch than the alternate root port, changing the port priority of the designated ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch stack. There is no workaround. (CSCea40988)
- 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

These are the VLAN limitations:

- 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)

- (Catalyst 3750 or 3560 switches) A CPUHOG message sometimes appears when you configure a private VLAN. Enable port security on one or more of the ports affected by the private VLAN configuration.

There is no workaround. CSCed71422

- (Catalyst 3750)

When you apply a per-VLAN quality of service (QoS), per-port policer policy-map to a VLAN Switched Virtual Interface (SVI), the second-level (child) policy-map in use cannot be re-used by another policy-map.

The workaround is to define another policy-map name for the second-level policy-map with the same configuration to be used for another policy-map. (CSCef47377)

## Device Manager Limitations and Restrictions

This release supports the same switch cluster compatibilities supported in Cisco IOS Release 12.1(22)EA1. However, you cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or the Cisco Network Assistant application. For information about Network Assistant, see the [“New Features” section on page 9](#).

## Important Notes

These sections describe the important notes related to this software release for the Catalyst 3750, 3560, and 2970 switches:

- [“Switch Stack Notes” section on page 22](#)
- [“Cisco IOS Notes” section on page 22](#)
- [“Device Manager Notes” section on page 23](#)

## Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- The Catalyst 3560 and 2970 switches do not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because these switches share common code with other switches that do support stacking.

## Cisco IOS Notes

These notes apply to Cisco IOS software:

- The 802.1x feature in Cisco IOS Release 12.1(14)EA1 and later is not fully backward-compatible with the same feature in Cisco IOS Release 12.1(11)AX. If you are upgrading a Catalyst 3750 or a 2970 switch running Cisco IOS Release 12.1(11)AX that has 802.1x configured, you must re-enable 802.1x after the upgrade by using the **dot1x system-auth-control** global configuration command. This global command does not exist in Cisco IOS Release 12.1(11)AX. Failure to re-enable 802.1x weakens security because some hosts can then access the network without authentication.

- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(18)SE and later. In Cisco IOS Release 12.1(19)EA and earlier, both of these command pairs disabled logging to the console:

- the **no logging on** and then the **no logging console** global configuration commands
- the **logging on** and then the **no logging console** global configuration commands

In Cisco IOS Release 12.2(18)SE and later, you can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)

## 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:

1. Choose **Tools > Internet Options**.
2. Click **Settings** in the “Temporary Internet files” area.
3. From the Settings window, choose **Automatically**.
4. Click **OK**.
5. Click **OK** to exit the Internet Options window.

- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

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

	Command	Purpose
Step 1	<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	<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.

- 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](http://www.cisco.com:84)), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.



# Open Caveats

These sections describe the open caveats with possible unexpected activity in this software release:

- [“Open IOS Caveats” section on page 25](#)
- [“Open Device Manager Caveats” section on page 28](#)

## Open IOS Caveats

Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Catalyst 3750, 3560, and 2970 switches:

- CSCeb42949 (Catalyst 3750 switches)  
A Catalyst 3750 switch does not work with the User Registration Tool (URT). The PC attempting to connect to the network can log in successfully, but it is not allowed to pass traffic after the port is moved to the user VLAN. The MAC address for that device shows *BLOCKED*.  
There is no workaround.
- CSCec68807 (Catalyst 3750 switches)  
Memory allocation (malloc) and remote-procedure call (RPC) throttle messages are sometimes displayed when a large number of access control lists (ACLs) are pasted to the console window.  
The workaround is to save the configuration and reload the switch stack.
- CSCec88895 (Catalyst 3750 switches)  
There is a discrepancy between the output of the **show controllers ethernet-controller tengigabitethernet1/0/1** and the **show interfaces tengigabitethernet1/0/1** privileged EXEC commands on a 10-Gigabit Ethernet interface.  
The workaround for 10-Gigabit Ethernet interfaces is to use the **show interface** privileged EXEC command for the byte count and the number of pause frames received. Use the **show controllers ethernet-controller** privileged EXEC command for the frame count and the FCS and CRC error-frame count.
- CSCed12889 (Catalyst 3750 switches)  
When redundant uplinks are from the same stack member in a switch stack and UplinkFast is configured, dummy multicast packets are not sent.  
The workaround is to not have redundant uplinks from the same stack member. Provide uplink connectivity from ports across the switch stack rather than from one switch in the stack.
- CSCed82005 (Catalyst 3750 or 3560 switches)  
If static IP source bindings are configured on an Etherchannel interface and the configuration is saved, the IP source bindings are lost when the switch is reloaded.  
There is no workaround.
- CSCed91730 (Catalyst 3750 switches)  
When a secondary VLAN is associated and then quickly disassociated, sometimes the MAC address tables across the switch stack become unsynchronized. This is a rare condition that happens when Port Fast is enabled on the host ports and traffic is continuously received on that port.  
The workaround is to clear the MAC address table by using the **clear mac address-table dynamic** privileged EXEC command.

- CSCed92268 (Catalyst 3750 or 3560 switches)

If a large per-port ACL (PACL) is configured on an interface and a TCAM full condition is created, entries corresponding to the IP source guard configuration are not programmed into the TCAM. If you remove the PACL, the IP source guard entries are still not programmed into the TCAM.

There is no workaround.

- CSCee07107 (Catalyst 3750 switches)

ARP and reverse ARP (RARP) packets are not properly filtered by a configured VLAN map. If you enable a VLAN for dynamic ARP inspection and a VLAN map is applied to the VLAN, ARP and RARP packets received in that VLAN on stack member ports that should be dropped by the VLAN map are not dropped.

There is no workaround.

- CSCee08109

If a port-based ACL (PACL) is applied to an 802.1x-enabled port and the client is then disconnected from that port, the PACL is not removed from the port.

There is no workaround.

- CSCee12496

When the **interface range** interface configuration command is used to set a range of ports to trusted mode by using the **ip arp inspection trust** command and some of those ports are members of a channel-group, this error message might appear:

```
%PM-3-INTERNALERROR: Port Manager Internal Software Error (pd->physicalPort &&
pd->agPort == NULL: ../switch/pm/pm_port.c: 3865: pm_port_want_to_bundle)
```

There is no workaround.

- CSCee14018 (Catalyst 3750 or 3560 switches)

Port ACLs are not applied to IGMP control packets with IP options.

There is no workaround.

- CSCee22376

When an SNMP version 3 user is configured with the encrypted option and password, the switch reloads when the MIB object `usmUserAuthKeyChange` is set.

The workaround is to configure a user without the encrypted option. (For example, **snmp-server user username groupname v3 auth md5 password**.)

- CSCee28016 (Catalyst 3750 switches)

When 802.1x is enabled on a port, spanning-tree Port Fast is added to the interface configuration. However, the Port Fast configuration might not appear until a link up occurs, and it might not appear on remote ports in a Catalyst 3750 stack. This does not affect the functionality of the switch.

There is no workaround.

- CSCee37070

An 802.1x port in single-host mode with port security enabled goes into the `errdisable` state and displays the `%DOT1X-5-SECURITY_VIOLATION` message if another MAC is seen.

The workaround is to have only one device connected at a time while in single-host mode.

- CSCee83209 (Catalyst 3750 switches)  
When the **default interface** *interface-id* interface configuration command is entered on a tunnel interface, the configuration is not completely cleared.  
There is no workaround.
- CSCee88546 (Catalyst 3750 switches)  
After a stack master fail-over, any per-user access control lists (ACLs) applied on authenticated 802.1x ports might appear twice when you enter the **show ip access-list** privileged EXEC command.  
This occurs when the authenticated port is on a member switch that becomes the stack master during fail-over. The duplicate display does not affect the functional behavior of the ACL.  
There is no workaround.
- CSCee93822  
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.
- CSCef37624 (Catalyst 3750 switches)  
If you attempt to ping a Layer 3 interface that has a Network Address Translation (NAT) configuration, the ping fails.  
There is no workaround.
- CSCef37959 (Catalyst 3750 or 3560 switches)  
The switch does not generate an ARP request for the next policy-based routing (PBR) hop when it receives packets that should be policy routed. This occurs when the PBR next-hop interface is in a down state, the packets are routed by using the normal routing table, and then PBR next-hop interface goes up.  
The workaround is to configure static ARP for the PBR next hop.
- CSCef38683 (Catalyst 3750)  
If a secondary address is configured on an interface and a RIP or HSRP packet enters the interface around the time the configuration change was done, the packet might be looped twice in the software and will then be dropped. A syslog error message appears.  
This does not affect the switch functionality.  
There is no workaround.
- CSCef42632 (Catalyst 3750 switches)  
If you apply a per-VLAN QoS policer policy-map to a VLAN switched virtual interface (SVI) and the policy-map has a class-map that uses ACL that requires L4OP (GT LT port range), the policy-map would not be effective.  
The workaround is to use the equal (eq) operator instead for Layer 4 port matching, or use a port-based policy-map instead.

- CSCef58386 (Catalyst 3750 switches)

In a switch stack of nine switches, when there are 802.1x interfaces that are in an authorized state for the guest VLAN, as the stack member that was reloaded comes up and is initializing, the guest VLAN interfaces on the stack master and the stack member switches go down for awhile and then come back up. This problem does not occur every time a stack member reloads.

There is no workaround.

- CSCef65587

These error messages appear randomly:

```
%SYS-2-NOBLOCK: idle with blocking disabled. -Process= "hpm main process", ipl= 0,
pid= 62

-Traceback= 259CC0 251438 750244 661220 665774 6603CC 653750 6575B0 64FC44 651260
65DF58 4EC268 544300 4F5F64 4B433C 522508

*Sep 2 15:42:22: %SYS-2-BLOCKHUNG: Task hung with blocking disabled, value = 0x1.
-Process= "hpm main process", ipl= 0, pid= 62

-Traceback= 259CFC 251438 750244 661220 665774 6603CC 653750 6575B0 64FC44 651260
65DF58 4EC268 544300 4F5F64 4B433C 522508
```

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

- CSCin68965 (Catalyst 3750 or 3560 switches)

When two ports of a Cisco IP Phone are connected to a switch and the higher voice VLAN ID (VVID) is configured on the switch port to which port P3 of the Cisco IP Phone is connected, the phone displays the message *configuring IP* and halts.

These are the workarounds. Only one of these is necessary:

- Configure the higher VVID on port P1 of the Cisco IP phone.
- Connect only one port of the Cisco IP Phone to the switch.

## Open Device Manager Caveats

These are the severity 3 device manager caveats for this release:

- CSCef45718

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.

- CSCef78853

Entering certain characters in some menu items in the device manager window can cause the front panel of a switch to not appear or error dialogs to appear. This can occur when a semicolon (;), single quotation mark ('), or double quotation mark (") is used as part of the hostname, port description, SNMP system location, SNMP system contact, SNMP community strings, Telnet password, or switch password.

The workaround is to remove the character from names of these menu items.

## Resolved Caveats

Unless otherwise noted, these caveats were resolved in this release for the Catalyst 3750, 3560, and 2970 switches:

- CSCed23767

The **switchport port-security aging time 0** interface configuration command now disables the aging time.

- CSCed37222

Sticky addresses are no longer lost during a master switchover.

- CSCed46781

If you configure the **dot1x timeout tx-period** interface configuration command as greater than **dot1x timeout quiet-period** interface configuration command, users are not authenticated into the guest VLAN when 802.1x authentication fails.

- CSCed65309 (Catalyst 3750 or 3560 switches)

Incoming invalid ARP packets are now dropped on dynamic ARP inspection-enabled VLANs.

- CSCed65410 (Catalyst 3750 or 3560 switches)

If dynamic ARP inspection is enabled on an internal VLAN used by a routed port, ARP traffic on the routed port is no longer affected by the dynamic ARP inspection processing. For example, ARP packets are no longer rate-limited.

- CSCed74349 (Catalyst 3750 switches)

It is no longer necessary to use physical ports on the stack master for any EtherChannel that carries dynamic ARP inspection VLANs and has rate limits. In previous releases, an EtherChannel was not properly error-disabled if these conditions were true:

- The channel is carrying a VLAN that is enabled for dynamic ARP inspection.
- The channel is configured with a rate limit for dynamic ARP inspection.
- At least one of the ports in the channel is on a stack member.
- ARP packets are received on a port in the channel on a stack member *at a higher rate* than the configured rate limit for the channel.

- CSCed78149

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCed87243

If the VTP password is configured but the VTP domain name is not configured, and if the switch reloads twice, the switch now retains the VLAN information.

- CSCed94657 (Catalyst 3750 or 3560 switches)

If a secondary VLAN that was mapped to a promiscuous port is disassociated from the primary VLAN, the LED on the promiscuous port no longer turns from green to amber. In previous releases, the LED of the promiscuous port turned from green to amber if the secondary VLAN was disassociated from the primary VLAN and also if the secondary VLAN was deleted.

- CSCee11197 (Catalyst 3750 switches)

You can now enter a value ranging from 1 to 4095 when configuring the VLAN for an access port from SNMP by using the `vlanPortVlan` object of the `CISCO-STACK-MIB`. In previous releases, you could only enter values ranging from 1 to 1023.

- CSCee14293 (Catalyst 3750 or 3560 switches)

The forwarding behavior for a multicast group is now correct if that group exceeds the maximum number that a private VLAN can support. When multicast routing is disabled, 500 groups are supported.

- CSCee14673 (Catalyst 3750 switches)

The switch no longer continuously displays this message:

```
%LINK-3-BADMACREG: Interface StackPort1, non-existent MACADDR registry for link 0
-Process= "<interrupt level>", ipl= 4-Traceback= 20AC84 188828 58ACCC 588F20 2D8020
2E00B4 2E2B80 2E2EAC 2B14E8
```

- CSCee30022

This message no longer appears when you add an aggregate policer to a policy map:

```
BAD policymap info 9999999
```

- CSCee30090

This message no longer appears when you modify a policer or remove an aggregate policer:

```
Download failed for <class-name>
```

```
Bad policymap info.
```

- CSCee30129

When you add an aggregate policer to a policy-map class, the aggregate policer is no longer also added to another policy class within the same policy.

- CSCee37552

The switch no longer fails when it executes the **shutdown** interface configuration command on an 802.1x enabled port.

- CSCee41566 (Catalyst 3750 switches)

Auto-upgrade no longer fails under either of these conditions:

- The stack is running a cryptographic image and a version-mismatch member switch that is running a noncryptographic image of the same type (both are EMI or SMI) joins the stack, or the reverse.
- If the stack is running a Cisco IOS 12.1 crypto image and a member switch running a Cisco IOS 12.2 crypto image of the same type joins the stack, or the reverse.

You no longer need to manually upgrade the member switch to run a compatible Cisco IOS image except under these conditions:

- If the stack master is running any Cisco IOS Release 12.1E cryptographic image and the member switch is running any noncryptographic image
- If the stack master is running any Cisco IOS Release 12.1E noncryptographic image and the member switch is running any cryptographic image
- If the stack master is running any Cisco IOS Release 12.1E cryptographic image and the member switch is running a 12.2S cryptographic image earlier than Release 12.2(25)SE
- If the stack master is running a Cisco IOS Release 12.2S cryptographic image earlier than Release 12.2(25)SE and the member switch is running any noncryptographic image
- If the stack master is running a Cisco IOS Release 12.2S noncryptographic image earlier than Release 12.2(25)SE and the member switch is running any cryptographic image
- If the stack master is running any Cisco IOS Release 12.2S cryptographic image earlier than Release 12.2(25)SE and the member switch is running any 12.1E cryptographic image
- If there is insufficient space for the new image

- CSCee53804 (Catalyst 3750 or 3560 switches)

When enabled, DHCP snooping now works with the secondary VLANs of a private VLAN. In previous releases, DHC- discovered messages from the private-VLAN hosts were not broadcast, and private-VLAN hosts could not communicate with the DHCP server.

- CSCee75231 (Catalyst 3750-G12S switches)

You can now use the Mode button to detect the presence of a switch stack member if a small form-factor (SFP) module is not in the module slot for that port on the member.

- CSCee75389 (Catalyst 3750 switches)

Reloading the stack master no longer causes its SFP ports to become unable to link up after the old stack master comes up as a member switch.

- CSCee84918

When DHCP snooping is enabled on the switch and clients attached to an interface move from one subnet to another, if a client attached to the switch sends a DHCP request to the previous subnet, the DHCP negative acknowledgement packet is no longer dropped by the switch.

- CSCee89040 (Catalyst 3750 switches)

When a local network link comes up, a MAC address that is defined in the static ARP table now installs the adjacency table immediately, and there is no temporary Cisco Express Forwarding (CEF) drop.

- CSCef04854

If you use the **no switchport** interface configuration command to configure a port as a routed port and then enable 802.1x on the port by using the **dot1x port-control auto** interface configuration command, 802.1x authentication no longer fails if you disable and then re-enable 802.1x on the port.

- CSCef09489

The switch now correctly forwards Extensible Authentication Protocol (EAP) messages received from a RADIUS server to a client with no delay to the client.

- CSCef16610

When IP source guard is configured and unconfigured on an interface several times, a memory leak no longer occurs.

- CSCef42734

When a new 802.1x session is started, the switch now purges old state information, which prevents the switch from failing to authenticate due to stale State(24) field values.

- CSCef55486

When the 802.1x accounting feature is configured, the switch no longer loses connectivity to the RADIUS server for an extended period of time, 802.1x transactions no longer time out, and switch reloads no longer occur.

- CSCef58927 (Catalyst 3750)

A switch no longer reloads under these conditions:

- The switch is configured for DHCP snooping database access.
- The switch accesses an FTP server.
- The switch accesses a DHCP snooping database file that is 0 bytes.

- CSCeg08820 (Catalyst 3750 or 3560 switches)

If a DHCP server is option-82 enabled, the server now correctly assigns an IP address to the interface when DHCP snooping, port security, and IP source guard are configured at the same time on the interface.

## Documentation Updates

This section provides updates to the product documentation.

- [“Correction to the Catalyst 3750 and 3560 Software Configuration Guides” section on page 33](#)
- [“Getting Started Guide” section on page 33](#)
- [“Regulatory Compliance and Safety Information Guide” section on page 33](#)
- [“Documentation Flyer” section on page 33](#)
- [“Hardware Installation Guide” section on page 34](#)



## Correction to the Catalyst 3750 and 3560 Software Configuration Guides

In the “Configuring HSRP Priority” section of the “Configuring HSRP” chapter of the Catalyst 3750 and 3560 software configuration guides, this information is incorrect in the procedure to configure HSRP priority characteristics on an interface:

In Step 3 and Step 4, the range for the **delay delay** keyword is 36000 (1 hour).

This is the correct information:

In Step 3 and Step 4, the range for the **delay delay** keyword is 3600 (1 hour).

## Getting Started Guide

The getting started guide is new to the Catalyst 3750, 3560, and 2970 documentation sets. The guide provides instructions on configuring the switch through the Express Setup program and on displaying or accessing the switch management interfaces, including the device manager. Switch management options, basic rack-mounting procedures, port and module connections, power-connection procedures, and troubleshooting help are also described in the guide.

The guide ships with the switches. It is also orderable from Cisco.com and is available on the Catalyst 3750, 3560, and 2970 documentation sites on Cisco.com.

**Note**

This guide replaces the information previously contained in the “Quick Setup” chapter in the switch hardware installation guide.

## Regulatory Compliance and Safety Information Guide

The regulatory compliance and safety information guide is new to the Catalyst 3750, 3560, and 2970 documentation sets. It contains agency approvals, compliance information, and translated warning statements.

This guide ships with the switch. It is also orderable from Cisco.com and is available on the Catalyst 3750, 3560, and 2970 documentation site on Cisco.com.

**Note**

This guide replaces the information previously contained in the “Translated Safety Warnings” appendix in the switch hardware installation guide.

## Documentation Flyer

The documentation flyers—which described where to find the Catalyst 3750, 3560, and 2970 documentation on Cisco.com—no longer ships with the switch. This information is now available in the new switch getting started guide (see [“Getting Started Guide” section on page 33](#)).

## Hardware Installation Guide

These changes have been made to the switch hardware installation guides:

- The switch hardware installation guide no longer ships with the switch. It is available on the Catalyst 3750, 3560, and 2970 documentation sites on Cisco.com.
- The “Quick Setup” chapter has been removed from this guide. Quick setup information, such as how to use the Express Setup program and how to display the device manager, is now available in the new switch getting started guide (see the [“Getting Started Guide” section on page 33](#)).
- The “Translated Safety Warnings” appendix has been removed from this guide. The translated safety warnings are now in the new regulatory compliance and safety information guide (see the [“Regulatory Compliance and Safety Information Guide” section on page 33](#)).

## Related Documentation

These documents provide complete information about the Catalyst 3750, 3560, and 2970 switches and are available at Cisco.com:

- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm>
- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3560/index.htm>
- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/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 35](#).

These documents provide complete information about the Catalyst 3750 switches:

- *Catalyst 3750 Switch Software Configuration Guide* (order number DOC-7816180=)
- *Catalyst 3750 Switch Command Reference* (order number DOC-7816181=)
- *Catalyst 3750 Switch System Message Guide* (order number DOC-7816184=)
- Device manager online help (available on the switch)
- *Catalyst 3750 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Getting Started Guide* (order number DOC-7816663=)
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch* (order number DOC-7816664)

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide* (order number DOC-7816404=)
- *Catalyst 3560 Switch Command Reference* (order number DOC-7816405=)
- *Catalyst 3560 Switch System Message Guide* (order number DOC-7816406=)
- Device manager online help (available on the switch)
- *Catalyst 3560 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3560 Switch Getting Started Guide* (order number DOC-7816660=)
- *Regulatory Compliance and Safety Information for the Catalyst 3560 Switch* (order number DOC-7816665)

These documents provide complete information about the Catalyst 2970 switches:

- *Catalyst 2970 Switch Software Configuration Guide* (order number DOC-7816182=)
- *Catalyst 2970 Switch Command Reference* (order number DOC-7816183=)
- *Catalyst 2970 Switch System Message Guide* (order number DOC-7816185=)
- Device manager online help (available on the switch)
- *Catalyst 2970 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2970 Switch Getting Started Guide* (order number DOC-7816685=)
- *Regulatory Compliance and Safety Information for the Catalyst 2970 Switch* (order number DOC-7816686=)

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 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/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

## Documentation Feedback

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

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

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

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

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

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

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

**Note**

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

## Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

# Obtaining Additional Publications and Information

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

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

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

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

<http://cisco.com/univercd/cc/td/doc/pcat/>

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

<http://www.ciscopress.com>

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

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

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

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

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

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

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

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

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

CCSP, 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, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0411R)

Copyright © 2004-2005 Cisco Systems, Inc. All rights reserved.