Release Notes for the Catalyst 2970 and Catalyst 3750 Switches, Cisco IOS Release 12.2(18)SE

Revised April 21, 2004

The Cisco IOS Release 12.2(18)SE runs on all Catalyst 2970 and Catalyst 3750 switches.

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

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, refer to 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, refer to the software upgrade filename for the software version.

For the complete list of Catalyst 2970 and Catalyst 3750 switch documentation, see the "Related Documentation" section on page 30.

You can download the switch software from these sites:

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

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

  (for nonregistered Cisco.com users)

This 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.

CISCO SYSTEMS

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

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

Note If you are upgrading a switch running Cisco IOS Release 12.1(11)AX that 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 19.

Contents

This information is in the release notes:

- "System Requirements" section on page 2
- "Downloading Software" section on page 5
- "Installation Notes" section on page 8
- "New Features" section on page 8
- "Limitations and Restrictions" section on page 9
- "Important Notes" section on page 18
- "Open Caveats" section on page 20
- "Resolved Caveats" section on page 24
- "Documentation Updates" section on page 29
- "Related Documentation" section on page 30
- "Obtaining Technical Assistance" section on page 32

System Requirements

The system requirements are described in these sections:

- "Hardware Supported" section on page 2
- "Cluster Compatibility" section on page 3
- "Software Compatibility" section on page 4

Hardware Supported

Table 1 lists the hardware supported by this software release.

Table 1 Catalyst 2970 and Catalyst 3750 Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
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[1] module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-12S	12 SFP 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

Table 1 Catalyst 2970 and Catalyst 3750 Supported Hardware (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
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[2] 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
SFP modules	1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, and CWDM[3]	–
Redundant power systems	Cisco RPS 300 Redundant Power System Cisco RPS 675 Redundant Power System	–

1. SFP = small form-factor
2. PoE =Power over Ethernet
3. CWDM = Coarse Wave Division Multiplexer

Cluster Compatibility

This section describes how to choose command and standby command switches when a cluster consists of a mixture of Catalyst switches. When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, Cisco recommends configuring the highest-end switch in your cluster as the command switch. Table 2 lists the cluster capabilities and Cisco IOS releases for the switches. The switches are listed from highest to lowest end.
- If you are managing the cluster through CMS, the switch that has the latest software should be the command switch, *unless* your command switch is running Cisco IOS Release 12.1(19)EA1 or later.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 switches.

Table 2 Switch Software and Cluster Capability

Switch	Cisco IOS Release	Cluster Capability
Catalyst 3750	12.1(11)AX or later	Member or command switch
Catalyst 3560	12.1(19)EA1b or later	Member or command switch
Catalyst 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX or later	Member or command switch
Catalyst 2955	12.1(12c)EA1 or later	Member or command switch

Table 2 Switch Software and Cluster Capability (continued)

Switch	Cisco IOS Release	Cluster Capability
Catalyst 2950	12.1(5.2)WC(1) or later	Member or command switch
Catalyst 2950 LRE	12.1(11)JY or later	Member or command switch
Catalyst 2940	12.1(13)AY or later	Member or command switch
Catalyst 3500 XL	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	11.2(8.5)SA6 (recommended)	Member switch only[1]
Catalyst 1900 and 2820	9.00(-A or -EN) or later	Member switch only

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

CMS is not forward-compatible on command switches running Cisco Release IOS 12.1(14)EA1 and earlier. This means that if a member switch is running a release that is earlier than the release running on the command switch, the new features are not available on the member switch. If the member switch is a new device running a release that is later than the release on the command switch, the command switch cannot recognize the member switch, and the Front Panel view displays it as an unknown device. You cannot configure any parameters or generate a report through CMS for that member; instead, you must launch the Device Manager application to configure and to obtain reports for that member.

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

Some early Cisco IOS releases do not support clustering.

For more information about clustering and CMS, refer to the software configuration guide.

Software Compatibility

For information about the recommended platforms for web-based management, operating systems and browser support, and CMS plug-in guidelines, refer to the “Getting Started with CMS” chapter of the software configuration guide.

Windows

This release uses a CMS plug-in to run CMS. You can download the latest CMS plug-in for Windows from this URL:

http://www.cisco.com/pcgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=windows&version=1.1

Solaris

This release uses a CMS plug-in that replaces the Java plug-in. You can download the latest CMS plug-in for Solaris from this URL:

http://www.cisco.com/pcgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=solaris&version=1.1

Downloading 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 CMS" section on page 6
- "Upgrading a Switch by Using the CLI" section on page 6
- "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. On Catalyst 3750 switches, the second line displayed in the output of the **show version** command shows C3750-I5-M for the enhanced multilayer image (EMI) or C3750-I9-M for the standard multilayer software image (SMI).

Note On Catalyst 3750 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 (SMI or EMI) and does not change if you upgrade the software image.

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

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 both the Cisco IOS image file and the files needed for CMS. You must use the combined tar file to upgrade the switch through CMS. To upgrade the switch through the CLI, use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the filenames for this software release.

Table 3 Cisco IOS Software Image Files

Filename	Description
c2970-i6l2-tar.122-18.SE.tar	Catalyst 2970 image file and CMS files. This image has Layer 2+ features.
c2970-i6k91l2-tar.122-18.SE.tar	Catalyst 2970 cryptographic image file and CMS files. This image has the Kerberos and SSH[1] features.
c3750-i9-tar.122-18.SE.tar	Catalyst 3750 SMI image file and CMS files. This image has the Layer 2+ and basic Layer 3 routing features.
c3750-i5-tar.122-18.SE.tar	Catalyst 3750 EMI image file and CMS files. This image has both the Layer 2+ and full Layer 3 routing features.
c3750-i9k91-tar.122-18.SE.tar	Catalyst 3750 SMI cryptographic image file and CMS files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3750-i5k91-tar.122-18.SE.tar	Catalyst 3750 EMI cryptographic image file and CMS files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.

1. SSH = secure shell

Upgrading a Switch by Using CMS

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

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 3 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 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 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 the **ping tftp-server-address** 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 the **archive download** 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-i9-tar.121-14.EA1.tar
```

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

Recovering from a Software Failure

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

Installation Notes

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

- The Express Setup program (refer to the hardware installation guide.)
- The CLI-based setup program (refer to the hardware installation guide.)
- The Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration (refer to the software configuration guide.)
- Manually assigning an IP address (refer to the software configuration guide.)

Note If you are upgrading a 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 19.

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

This release supports the Catalyst 3750-24PS and Catalyst 3750-48PS PoE switches. For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

For a list of default settings after initial switch configuration, including default settings that are changed in Cisco IOS Release 12.2(18)SE, refer to Table 1-1 in Chapter 1 of the software configuration guide.

For a list of commands that have the same function in Cisco IOS Release 12.1(19)EA1 or earlier but different syntax in Cisco IOS Release 12.2(18)SE, refer to Table 1-2 in Chapter 1 of the command reference.

Cisco IOS Release 12.2(18)SE contains these new features or enhancements:

- User-defined and Cisco-default Smartports macros for creating custom switch configurations for simplified deployment across the network.

Note Smartports macros are referred to as *SmartPort macros* in the software configuration guide and in the command reference.

- Support for the Catalyst 3750-24PS and the Catalyst 3750-24PS PoE switches. These switches can provide power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices from all 10/100 Ethernet ports if the switch detects that there is no power on the circuit.

- CMS support for the CMS plug-in that replaces the Java plug-in on Solaris systems. You must download the CMS plug-in to run CMS for this release.

  For more information about the CMS plug-in for Windows and Solaris systems, including the URLs, see the "Software Compatibility" section on page 4.

Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release required to support the major features of the Catalyst 2970 and 3750 switches.

Table 4 Catalyst 2970 and Catalyst 3750 Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
Smartports macros	12.2(18)SE

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.

These sections describe the limitations and restrictions:

- "Cisco IOS Limitations and Restrictions" section on page 9
- "Cisco IOS Limitations and Restrictions (Catalyst 3750 Switches Only)" section on page 13
- "Cluster Limitations and Restrictions" section on page 17
- "CMS Limitations and Restrictions" section on page 17

Cisco IOS Limitations and Restrictions

These limitations apply to Cisco IOS configuration on the Catalyst 2970 and Catalyst 3750 switches:

- "Configuration" section on page 10
- "HSRP" section on page 10
- "Ethernet" section on page 11
- "IP" section on page 11
- "IP Telephony" section on page 11
- "Multicasting" section on page 11
- "QoS" section on page 12
- "SPAN and RSPAN" section on page 12
- "Trunking" section on page 12
- "VLAN" section on page 13

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/CSCdz11708)

- Certain combinations of features and switches create conflicts with the port security feature. In Table 1, *No* means that port security cannot be enabled on a port on the referenced switch if the referenced feature is also running on the same port. *Yes* means that both port security and the referenced feature can be enabled on the same port on a switch at the same time. A dash means not applicable.

Table 5 Port Security Incompatibility with Other Switch Features

	Catalyst 2940	Catalyst 2950 and Catalyst 2955	Catalyst 2970	Catalyst 3550	Catalyst 3750
DTP[1] port[2]	No	No	No	No	No
Trunk port	No	No	Yes	Yes	Yes
Dynamic-access port[3]	No	No	No	No	No
Routed port	—	—	—	No	No
SPAN source port	Yes	Yes	Yes	Yes	Yes
SPAN destination port	No	No	No	No	No
EtherChannel	No	No	No	No	No
Tunneling port	—	—	—	Yes	—
Protected port	Yes	Yes	Yes	Yes	Yes
802.1x port	—	Yes[4]	Yes	Yes	Yes

1. DTP = Dynamic Trunking Protocol
2. A port configured with the **switchport mode dynamic** interface configuration command.
3. A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.
4. The switch must be running the enhanced software image (EI).

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 Protocol (STP) blocking state. To verify that these ports are not in the blocking state, refer to the "Configuring STP" chapter in the software configuration guide. (CSCec76893)

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)
- A Gigabit Ethernet connection between a SGMII (Serial Gigabit Media Independent Interface) port (3/4, 7/8, 11/12, 15/16, 19/20, and 23/24) and an Intel Pro/1000T Server Adapter NIC might lose connectivity on the Catalyst 3750G-24T and 3750G-24TS switches. The link activates correctly, but might subsequently stop exchanging data. This is an Intel product defect. The workaround is to use RGMII (Reduced Gigabit Media Independent Interface) ports (1/2, 5/6, 9/10, 13/14, 17/18, and 21/22) instead of SGMII ports. You can also use the **speed 1000** interface configuration command to force the speed of the port to 1000 Mbps. (CSCea77032)

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:

- 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 deleted manually or automatically when a topology 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)

QoS

This is the quality of service (QoS) limitation:

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)

SPAN and RSPAN

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

- 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. (CSCea72326)
- The Cisco Discovery Protocol (CDP), Virtual Terminal 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)

Cisco IOS Limitations and Restrictions (Catalyst 3750 Switches Only)

These limitations only apply to the Cisco IOS configuration on the Catalyst 3750 switches:

- "IP" section on page 13
- "Fallback Bridging" section on page 14
- "MAC Addressing" section on page 14
- "Multicasting" section on page 14
- "Routing" section on page 15
- "SPAN" section on page 15
- "Spanning Tree Protocol" section on page 16
- "Stacking" section on page 16

Configuration

These are the configuration limitations:

- 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:

a. Disable auto-QoS on the interface.

b. Change the routed port to a nonrouted port or the reverse.

c. Re-enable auto-QoS on the interface. (CSCec44169)

- 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)

IP

This is the IP limitation:

The switch does not create an adjacent table entry when the Address Resolution Protocol (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. (CSCe21674)

Fallback Bridging

These are the fallback bridging limitations:

- 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)
- 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)

MAC Addressing

This is the MAC addressing limitation:

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 multicast limitations:

- 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 on a trunk port in at least one VLAN, this problem for the non-RPF traffic occurs. (CSCdu25219)
- When you use the **ip access-group** interface configuration command with a router 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)
- 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)

Routing

These are the routing limitations:

- A route map that contains an ACL with a DSCP clause cannot be applied to a Layer 3 interface. The Catalyst 3750 rejects this configuration and displays the following an error message that the route map is unsupported. There is no workaround. (CSCea52915)
- If there are a large number of SVIs, routes, or both on a fully populated nine-member switch stack, the following error 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 which 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)
- A Catalyst 3750 switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.

SPAN

These are the SPAN 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. (CSCdy72835)
- 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 remote SPAN (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. (CSCdy81521)
- 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, 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 traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)

Spanning Tree Protocol

This is the STP limitation:

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)

Stacking

These are the stacking limitations:

- If the stack master is reloaded immediately 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)
- The Catalyst 3750 EMI cryptographic image has a higher priority than the Catalyst 3750 SMI image during the master switch election in a stack. When two or more switches in the stack use different software images, such as the SMI image for Cisco IOS Release 12.1(11)AX and the cryptographic EMI for Cisco IOS Release 12.1(19)EA1 or later, the switch running the SMI is selected as the stack master. This occurs because the switch running the cryptographic EMI takes 10 seconds longer to start than does the switch running the SMI. The switch running the EMI is excluded from the master election process that lasts 10 seconds.

  The workaround is to upgrade the switch running the SMI to a software release later than Cisco IOS Release 12.1(11)AX or to manually start the master switch and wait at least 8 seconds before starting the new member switch. (CSCec32137)
- 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)
- 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)

Cluster Limitations and Restrictions

These limitations apply to cluster configuration on the Catalyst 2970 and Catalyst 3750 switches:

- When there is a transition from the cluster active command switch to the standby command switch, Catalyst 1900, 2820, and 2900 4-MB switches that are cluster members might lose their cluster configuration. You must manually add these switches back to the cluster. (CSCds32517, CSCds44529, CSCds55711, CSCds55787, CSCdt70872)
- When a Catalyst 2900 XL or 3500 XL cluster command switch is connected to a Catalyst 3550 or to a 3750 switch, the command switch does not find any cluster candidates beyond the Catalyst 3550 or the 3750 switch if it is not a member of the cluster. You must add the Catalyst 3550 or the 3750 switch to the cluster. You can then see any cluster candidates connected to it. (CSCdt09918)
- If both the active command switch and the standby command switch fail at the same time, the cluster is not automatically recreated. Even if there is a third passive command switch, it might not recreate all cluster members because it might not have all the latest cluster configuration information. You must manually recreate the cluster if both the active and standby command switches simultaneously fail. (CSCdt43501)

CMS Limitations and Restrictions

These limitations apply to CMS configuration:

- CMS performance degrades if the Topology View is open for several hours on a Solaris machine. The cause might be a memory leak.

  The workaround is to close the browser, reopen it, and launch CMS again. (CSCds29230)
- If you are printing a Topology View or Front Panel View that contains many devices and are running Solaris 2.6 with JDK1.2.2, you might get an *Out of Memory* error message.

  The workaround is to close the browser, re-open it, and launch CMS again. Before you perform any other task, open the view that you want to print, and click Print in the CMS menu. (CSCds80920)
- A red border appears around the text-entering area of some CMS dialogs. The color of the border changes to green when text is entered. This is only a cosmetic error. The colored border does not prevent you from entering text. (CSCdv82352)
- You cannot switch modes (for example, from Guide Mode to Expert Mode) for an open CMS window.

  The workaround is to close the open window, select the mode that you want, and then reopen the CMS window. For the mode change to take effect on any other CMS window that is open, you need to close that window and then reopen it after you select the new mode. (CSCdw87550)
- If you open a window in which you can enter text, open another window, and return to the first window, right-clicking in the text field might make the cursor in this field disappear. You can still enter text in the field. (CSCdy44189)
- CMS fails when a switch is running the cryptographic software image and the vty lines have been configured to use only secure shell (SSH) using the **transport input ssh** and **line vty 0 15** global configuration commands.

  The workaround is to allow SSH and Telnet access through the vty lines by using the **transport input ssh telnet** and **line vty 0 15** global configuration command. (CSCdz01037)

- When you add a new member with a username and password that is different from the existing cluster member usernames and passwords, CMS produces an exception error because of an authentication failure.

  The workaround is to add the new member without any username and password. When the new member is added to the cluster, remove the existing username and password from the Username and Password fields, enter a new username and password, and then apply it to all cluster members. (CSCdz07957)
- When the Link Graphs application has run for hours displaying packet drop and error information, sometimes the X-axis crosses the Y-axis at a negative y value instead of at y = 0. This condition occurs with all supported operating systems, browsers, and Java plug-ins. There is no workaround. (CSCdz32584)
- After you click **Apply** or **Refresh** in the SNMP window, the window size changes. (CSCdz75666, CSCdz84255)
- When you enable log scaling for Link Graphs, the Y-axis scale becomes illegible. There is no workaround. (CSCdz81086)
- The CMS window does not return to full size after resizing the NE or IE when using Netscape version 6.xx on Solaris and Linux. This is a Netscape browser problem. There is no workaround. (CSCea01179)
- CMS sometimes halts after you click **Apply** when using Netscape 4.7 on the Japanese version of Windows 98 or Windows ME.

  The workaround is to use Microsoft Internet Explorer or Netscape 6.0 or later. (CSCea27408)
- Changing the password or current authentication while CMS is running causes HTTP requests to fail.

  The workaround is to close all browser sessions and then relaunch CMS. (CSCeb33995)
- When TACACS authentication is only enabled on a command switch, member switches cannot be configured.

  The workaround is to enable TACACS authentication on the member switches. (CSCed27723)
- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when also entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.
- ACEs that contain the **host** keyword precede all other access control entries (ACEs) in standard ACLs. You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.

Important Notes

These sections describe the important notes related to this software release:

- "Switch Stack Notes" section on page 19
- "Cisco IOS Notes" section on page 19
- "CMS Notes" section on page 19

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 2970 switch does not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because the Catalyst 2970 shares common code with other switches that do support stacking.

Cisco IOS Notes

This note applies 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 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.

CMS Notes

These notes apply to CMS configuration:

- If you use CMS on Windows 2000, it might not apply configuration changes if the enable password is changed from the CLI during your CMS session. You have to restart CMS and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- CMS does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using CMS, you cannot create classes that match more than one match statement. CMS does not display policies that have such classes.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.add.com*:84), you must enter *http://* as the URL prefix. Otherwise, you cannot launch CMS.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.
- If you have a proxy server configured on your web browser, CMS can run slowly and take 2 to 3 minutes to process each command that is entered.
- If you use the Netscape browser to view the CMS GUI and you resize the browser window while CMS is initializing, CMS does not resize to fit the window.

  The workaround is to resize the browser window again when CMS is not busy.

- In the Front Panel view or Topology view, CMS does not display error messages in read-only mode for these switches:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

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

Open Caveats

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

- "Open Cisco IOS Caveats" section on page 20
- "Open Cisco IOS Caveats (Catalyst 3750 Switches Only)" section on page 21
- "Open CMS Caveats" section on page 23

Open Cisco IOS Caveats

These are the severity 3 Cisco IOS configuration caveats on the Catalyst 2970 and Catalyst 3750 switches:

- CSCeb67510

  When both the sharing and shaping weights are enabled, the receiving rates might not follow the shared bandwidth weight if the priority queue is enabled on the egress queue.

  The workaround is to use lower values of the shaped and shared weights for queues other than the first queue when the egress priority queue is enabled and if shaping in other queues is required.

- CSCed04063

  When the **kerberos clients mandatory** global configuration command is entered on a switch and the switch is connected to a host that does not support Kerberos through a Telnet session, the switch might halt and then fail when the you press the Enter key.

  The workaround is to not use the **kerberos clients mandatory** global configuration command.

- CSCed18488

  When (*,G) and (S,G) entries are created in a multicast routing table on a remote port by Protocol-Independent Multicast-Sparse Mode (PIM-SM) registering, the RPF leak flag is not set for hardware entry for the group. This behavior causes high CPU utilization when the CPU receives non-RPF traffic in some topologies.

  The workaround is to configure the access list for the group to drop non-RPF traffic in hardware.

Open Cisco IOS Caveats (Catalyst 3750 Switches Only)

These open caveats only apply to the Catalyst 3750 switches.

- CSCea84802

  While booting up a nine-member switch stack with a large number of SNMP traps enabled, some of the stack members might not start up fully and become operational. There are two possible scenarios:

  – The stack member stays in the initializing state. Use the **show switch** user EXEC command to detect this condition. Normally a switch joining the switch stack transitions from `Initializing` to `Ready` within 1 minute.

  – The stack member start up in the ready state, but all ports on the stack member remain in the link down state even though link partners indicate a linkup state.

  The workaround is to reboot the whole switch stack using one of these methods:

  – Use the **reload** privileged EXEC command on the stack master.

  – Power cycle the stack master.

- CSCeb42949

  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.

- CSCeb49472

  Although visible in the command-line help string, the **source-only-learning** keyword is not supported on the Catalyst 3750 switches. The IGMP report-suppression feature is also not supported.

  There is no workaround.

- CSCeb66720

  When CDP is disabled on a stack member interface and that interface is converted to a routed port or switch port, CDP is re-enabled on the stack member interfaces. Having CDP enabled on a stack member but not on the stack master can cause the 802.1x voice VLAN features to fail on the stack member.

  The workaround is to enable and then disable CDP on the interface.

- CSCeb75366

  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.

- CSCec05769

  If the system frame size is configured by using the **system mtu jumbo** global configuration command, the switch does not consistently forward routed IP packets between 1518 and 2016 bytes. These packets might be forwarded or dropped.

  There is no workaround.

- CSCec89120

  The command switch sometimes does not discover candidates more than one CDP hop beyond its routed port.

  The workaround is to change the routed port to a switch port

- CSCed09484

  When a Type-1 Token Ring patch cable is connected to a PoE port on a Catalyst 3750 switch, the switch detects an error, but does not put the port into an error-disabled state.an error, but does not put the port into an error-disabled state.

  There is no workaround. However, when a valid link partner is connected to the PoE port, it operates normally and without user intervention.

- CSCed11059

  When Cross-Stack UplinkFast is configured, entering the **shutdown** and **no shutdown** interface configuration commands on one of the uplink ports might cause the uplink ports to be blocked in some VLANs for twice the forward-delay timer value.

  There is not workaround. The new root port will go to a forwarding state on its own after twice the forward delay value on the VLANs.

- CSCed12889

  Dummy multicast packets are not transmitted under these conditions:

  - The switches are in the same stack.
  - The redundant uplink ports are from the same switch.
  - Uplinkfast is configured.

  The workaround is to redundant uplinks configured on the same switch. Provide uplink connectivity from ports across the stack rather than from one switch in the stack.

- CSCed30095

  A topology change on a member switch might not cause fast-aging of the dynamically-learned addresses. This occurs in PVST mode when a topology change notification (TCN BPDU) that is generated and propagated from a member switch is not sent out of the root port on the master. Because the root bridge does not receive the TCN, it cannot cause all the bridges in the network to reduce their aging time to forward-delay time. As a result, there might be a connectivity outage for as long as the mac-address aging time.

  There is no workaround.

- CSCed33792

  Members of a stack might fail after the debug all members can crash when **debug all** privileged EXEC is entered.

  The workaround is to not enter the **debug all** comment. Only enable relevant debugs.

- CSCed34921

  If there is a Layer-3 (routed port) LACP EtherChannel on the stack master, changing the LACP system-priority, either locally or on the neighbor switch, creates assert failure and traceback error messages for the ports in the EtherChannel.

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

- CSCed39178

  When an RSPAN destination session is configured on a Catalyst 3750 switch, multicast traffic is not forwarded to the destination port. Unicast traffic is received correctly.

  There is no workaround

- CSCed54175

  The Catalyst (3550/2950/2970/3750) switch does not accept duplicate remark statements in named ACLs.

  There is no workaround.

Open CMS Caveats

These are the severity 3 CMS configuration caveats:

- CSCec18805

  When you launch the IP Multicast wizard, multicast-enabled devices do not appear in the list of multicast-enabled devices.

  There is no workaround. The wizard does not display multicast-enabled devices.

- CSCec61919

  The Topology View does not show unknown devices or devices that are down.

  There is no workaround.

- CSCed21655

  The CMS plug-in is not supported in Netscape 4.7x.

  The workaround is to use a supported browser, such as Netscape 7.1 or Internet Explorer 5.5 or 6.0.

- CSCed34582

  The Front Panel View sometimes does not show the port LED status.

  The workaround is to refresh the Front Panel View.

- CSCed39693

  When there are Catalyst 2950 and 2955 devices in a cluster, if you launch the QoS Queue Window to configure the devices and then try to view the settings for other devices by using the device selection menu, CMS halts after 20 to 30 selections.

  The workaround is to close CMS and then restart CMS.

- CSCed40866

  If an ACL is deleted from a device, all QoS classes that use this ACL for traffic classification become unusable (only on Catalyst 2970 and 3750 switches). The modification of these classes to use any other traffic classification (match statement) fails.

  The workaround is to delete the QoS class that uses the undefined ACL and then recreate it with the intended traffic classification (match statement).

Resolved Caveats

These are the caveats that have been resolved in this release.

- "Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(18)SE" section on page 24
- "Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(18)SE (Catalyst 3750 Switches Only)" section on page 27
- "Cisco CMS Caveats Resolved in Cisco IOS Release 12.2(18)SE" section on page 28

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(18)SE

These Cisco IOS caveats were resolved in Cisco IOS Release 12.2(18)SE:

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCdz30046

  When multicast VLAN registration (MVR) groups are added or deleted, the receiver port that joined the groups after the addition no longer receives traffic after the group is deleted. MVR data traffic to the group is no longer sent to the receiver port immediately after the **no mvr group** *ip-address* global configuration command is entered.

- CSCeb05183

  The Port Settings table no longer displays meaningless information in the columns for interface description and duplex cells. This problem occurred for some of the Catalyst 2820 and Catalyst 1900 switches.

- CSCeb56226

  It is no longer necessary to restart a port by using the **shutdown** and **no shutdown** interface configuration commands after you remove a voice VLAN and disable 802.1x on that port.

- CSCeb66606

  When DHCP snooping is enabled and the lease time given by the server to the client is infinite, tracebacks are no longer generated.

- CSCec07637

  When an ACL that denies packets is configured on an ingress or egress interface, the CPU usage is no longer as high as 70 percent when these packets are forwarded to the CPU to determine if an ICMP-unreachable packet should be generated.

- CSCec11048

  When a configured secure MAC address exists on an interface, you can now change it to a sticky MAC address. Alternatively, if a sticky MAC address exists on an interface, you can now change it to a secure MAC address.

- CSCec21320

  After a link is up, a switch sends three Extensible Authentication Protocol (EAP) Request/Identity messages to the client. There is a 30-second gap between messages. However, PCs that are running Windows XP or Windows 2000 drop the first message so that the second message that the client receives *appears* to be the first, which is at least 30 seconds after the link is up. Therefore, a user does not see a password window until at least 30 seconds after the link is up.

- CSCec82728

  When using Rapid PVST+ or MSTP, a transient-spanning-tree loop no longer occurs when the network reconverges after the spanning-tree root VLAN has aged out.

- CSCed11323

  If there are multiple aggregate policers configured on a switch and one of the policers is used in a policy map that has been applied to an interface, the switch no longer fails if you remove the aggregate policer without first detaching it from the policy map. In previous releases, this occurred when you first applied the command or after you saved the configuration and then reloaded the switch

- CSCec12147

  When the CISCO-STP-EXTENSIONS-MIB is polled, unknown indexes are no longer returned for some MIB objects.

- CSCec21040

  When an 802.1x-enabled port is authenticated with a RADIUS-assigned VLAN, if the port is shut down or the link is removed, a traceback message no longer appears.

- CSCec22431

  Telnet and ping traffic is no longer disrupted during SNMP polling of the VlanTrunkPortTable table in the CISCO-VTP-MIB.

- CSCec22572

  When per-user access control lists (ACLs) are downloaded from a RADIUS server after successful 802.1x authentication, disabling 802.1x now removes the attached per-user ACLs from the interface.

- CSCec27421

  If QoS is enabled and the trust state is not configured on an ingress interface, now only the mapping of the class of service (CoS) value of 0 to the ingress or egress queues takes effect when you enter the **mls qossrr-queue input cos-map** or the **mls qos srr-queue output cos-map** global configuration command. Other CoS values DSCP values to queue mapping have no effect on traffic from that interface.

- CSCec31436

  When there are many configured secure and sticky MAC addresses on a port, addresses are no longer dropped and removed from the configuration when the switch restarts.

- CSCec32453

  When you configure a unicast MAC address filter that matches a Windows XP 802.1x client MAC address, the Windows XP 802.1x client now no longer repeatedly tries to re-authenticate itself.

- CSCec49525

  Information is now correctly logged when ACL logging option is enabled.

- CSCec54619

  When two ports on a Catalyst 3750 switch are connected back-to-back in Rapid-PVST+ or MST mode, the **show spanning-tree** user EXEC commands no longer show the role of the backup port as *alternate* if the root port of the switch is a stack port.

- CSCec55073

  If you paste a configuration that has a large ACL into the running configuration of a Catalyst 3750 switch, the console no longer halts, and the switch no longer fails.

- CSCec82690

  When a topology change bridge occurs, bridge protocol data units (BPDUs) are now sent from an RSTP switch that is communicating with a per-VLAN PVST+ switch. The MAC tables on a PVST+ switch are also now cleared after a topology change.

- CSCec71526

  When an HSRP standby device is the cluster commander and the HSRP group is bound to the cluster, the active device now always shows greater than zero members when the **show cluster** user EXEC command is entered. The standby device now recognizes all of the cluster members, so if the active device fails, the standby device successfully takes over as the command switch.

- CSCec87974

  When you use SNMP to poll a switch, the ifHCInOctets/ifHCOutOctets 64 bit counters in the ifXTable no longer display 0 for Gigabit EtherChannel interfaces.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(18)SE (Catalyst 3750 Switches Only)

These Cisco IOS caveats on the Catalyst 3750 switches were resolved in Cisco IOS Release 12.2(18)SE:

- CSCeb14406

  IP multicast packets are now correctly forwarded over Distance Vector Multicast Routing Protocol (DVMRP) tunneled interfaces.

- CSCeb29898

  After booting up a switch stack that has more than 300 VLANs and the maximum number of static EtherChannel groups (12), all interfaces that are part of an EtherChannel no longer stay down.

- CSCeb37125

  Fallback bridging now works correctly when the TCAM is full, the switches in the stack have routed ports in the bridge group, and a switch is added or deleted from the switch stack.

- CSCeb40267

  If a Catalyst 3750 switch is added as a member to a stack of switches, and that new member switch is running a different Cisco IOS release than the rest of the stack, the switch is put into a *version mismatch* state as expected. However, the switch no longer reloads when the CISCO-FLASH-MIB is polled by SNMP.

- CSCeb42953

  If a Cisco IP Phone is connected to a port on the stack master, and 802.1x port security and voice VLAN are configured on the port, disabling port security no longer deletes the IP Phone MAC address from the MAC address table on all stack members.

- CSCeb69078

  Entering remote commands on a Catalyst 3750-12S switch that is unpacking and copying a new software image to flash memory no longer causes the software upgrade to fail.

- CSCeb73584

  If a stack of Catalyst 3750 switches has a running configuration file larger than 400 kilobytes, this error message no longer appears when you exit global configuration mode and every 30 seconds while you are in global configuration mode:

  ```
  PLATFORM_RPC-3-UNABLE_TO_SEND:System is unable to send RPC message:fifo full,
  paks_outstanding:256
  -Traceback= 607734 6028FC 602BD4 604A40 603E10 60AC94 60AD98 60BA28 1DF7FC
  ```

- CSCec29970

  If you change the input priority queue for queue 2 by using the **mls qos srr-queue input priority-queue 2 bandwidth** global configuration command, the configurations that are generated no longer contain an extra **input** keyword such as **mls qos srr-queue input priority-queue input 2 bandwidth**. In previous releases, the extra keyword caused an error message if the command was saved and the switch was reloaded.

- CSCec35148

  Processor memory no longer leaks if you change the policy-based routing (PBR) configuration.

- CSCec55847

  When a stack is started in per-VLAN Spanning Tree plus (PVST+) or Rapid-PVST+ mode with more than 128 VLANs, the spanning-tree instance created for the specified VLAN now includes ports on the member switches when these steps are followed:

a. The **spanning-tree vlan** *vlan-id* global configuration command is entered for the 129th VLAN. As expected, no STP instance is created.

b. One or more of the existing spanning-tree instances is deleted.

c. The **spanning-tree vlan** *vlan-id* global configuration command is entered for the same VLAN (as in step 1 above). As expected, an STP instance is now created. But this instance does not include ports on the member switches.

- CSCec59254

  A Catalyst 3750 switch now floods group- and source-specific queries to all ports of a VLAN.

- CSCed29169

  The IGMP maximum query response time is no longer set to 1 second. You can configure this value by using the **ip igmp query-max-response-time** *seconds* interface configuration command.

- CSCed33857

  A switch stack now forwards frames over an EtherChannel when the physical links of the EtherChannel are on a member switch. In previous releases, the stack did not forward frames when the EtherChannel was configured as a trunk and the stack was running IEEE 802.1S Multiple STP (MSTP) mode.

Cisco CMS Caveats Resolved in Cisco IOS Release 12.2(18)SE

These CMS caveats were resolved in Cisco IOS Release 12.1(20)EA1:

- CSCeb23334

  CMS now recognizes 802.1t spanning-tree extensions and port-priority configuration values under the STP Port Parameters tab, and they are now validated before they are added to the switch.

- CSCeb23416

  CMS now validates STP path-cost configuration values against the valid value ranges before they are added to the switch.

- CSCeb23592

  CMS now recognizes 802.1t spanning-tree extensions and bridge-priority configuration values under the STP Bridge Parameters tab, and they are now validated before they are added to the switch.

- CSCeb40625

  Shaped bandwidth weights are invalid if either the sum of their reciprocals is greater than one, or if the sum of their reciprocals is equal to one and the shaped weight of the queue is zero. CMS now detects these invalid bandwidth weights.

- CSCec08618

  CMS now recognizes 802.1t spanning-tree extensions and port-priority configuration values under the STP Port Parameters tab, and they are now validated before they are added to the switch.

- CSCec08662

  If UplinkFast is enabled and you enter a value in the Path Cost field in the STP Modify Port Parameters window, 3000 is automatically added to the configured-STP cost value. For example, if the path cost is 10, the actual value becomes 3010. If you disable UplinkFast, the path-cost value changes to its originally configured value of 10.

- CSCec09433

  You can now attach or remove an access control list (ACL) to or from an interface when you are in Guide Mode.

- CSCec16057

  CMS now recognizes the Coarse Wave Division Multiplexer (CWDM) small form-factor pluggable (SFP) module on Catalyst 2940 switches.

- CSCec34831

  When you click the **Highlight VLAN Port Membership Modes** button in the VLAN window of a switch, and that switch front panel is not displayed in Front Panel View, CMS brings the Front Panel View to the foreground. The front panel view of the switch is now displayed, and you can see the highlighted ports.

- CSCec45975

  In an AVVID wizard **Save Configuration** window step, an error message no longer appears if you click the Previous button.

- CSCec47247

  The IGMP Report Window now lists all the entries in the table.

Documentation Updates

This section provides these updates to the product documentation:

- "Correction to the Catalyst 2970 and Catalyst 3750 Hardware Installation Guides" section on page 29
- "Correction to the Catalyst 2970 and Catalyst 3750 Switch Software Configuration Guides" section on page 30
- "Correction to the Catalyst 2970 and Catalyst 3750 Switch Command References" section on page 30

Correction to the Catalyst 2970 and Catalyst 3750 Hardware Installation Guides

This is a new step for the "Configuring the Switch Settings" section in the "Using Express Setup" chapter:

Step 2

Enter a VLAN ID in the **Management Interface (VLAN ID)** field. This is the management interface through which you manage the switch and to which you assign IP information. The Management Interface field displays **1** by default. The VLAN ID range for this field is 1 to 1001.

Correction to the Catalyst 2970 and Catalyst 3750 Switch Software Configuration Guides

This correction is for the "Configuring SmartPort Macros" chapter in the software configuration guides:

SmartPort macros are now referred to as *Smartports macros*.

Correction to the Catalyst 2970 and Catalyst 3750 Switch Command References

This correction is for the command references:

- To disable secure address aging, use the **no switchport port-security aging time** interface configuration command. In previous releases, secure address aging was disabled by using the **switchport port-security aging time 0** interface command. This command is no longer available in the CLI.
- The command references incorrectly state that both of these sets of commands can be entered to disable 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.

Related Documentation

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

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 31.

- *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=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2970 Switch Hardware Installation Guide* (order number DOC-7815469=)

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

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 31:

- *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=)

- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 3750 Switch Hardware Installation Guide* (order number DOC-7815136=)

For other information about related products, refer to these documents:

- *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 provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

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

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

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

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

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

Click Subscriptions & Promotional Materials in the left navigation bar.

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

You can submit e-mail comments about technical documentation to 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, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:

  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 online at this URL:

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

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

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, 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. (0401R)

This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at

http://oss.software.ibm.com/icu4j/

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