



# Release Notes for the Catalyst 3750 Metro Switch Cisco IOS Release 12.2(25)EY and Later

---

Revised January 24, 2007

These release notes include important information about Cisco IOS Release 12.2(25)EY, Cisco IOS Release 12.2(25)EY1, Cisco IOS Release 12.2(25)EY2, Cisco IOS Release 12.2(25)EY3, and Cisco IOS Release 12.2(25)EY4, and any limitations, restrictions, and caveats that apply to the releases. 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 3.
- 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 3.

For the complete list of switch documentation, see the “[Related Documentation](#)” section on page 30.

You can download the switch software from this site:

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

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

Cisco IOS Release 12.2(25)EY and later are based on Cisco IOS Release 12.2(25)S. Use this document with the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/122srn.htm>

## Contents

This information is in the release notes:

- “[Hardware Supported](#)” section on page 2
- “[Uploading the Switch Software](#)” section on page 3



---

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

© 2005 Cisco Systems, Inc. All rights reserved.

- [“Installation Notes” section on page 5](#)
- [“New Features” section on page 5](#)
- [“Minimum Cisco IOS Release for Major Features” section on page 6](#)
- [“Limitations and Restrictions” section on page 7](#)
- [“Important Notes” section on page 15](#)
- [“Open Caveats” section on page 16](#)
- [“Resolved Caveats” section on page 19](#)
- [“Documentation Updates” section on page 28](#)
- [“Related Documentation” section on page 30](#)
- [“Obtaining Documentation” section on page 30](#)
- [“Obtaining Technical Assistance” section on page 32](#)
- [“Obtaining Additional Publications and Information” section on page 34](#)

## Hardware Supported

Table 1 lists the supported hardware and the minimum Cisco IOS release required.

**Table 1** Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750 Metro 24-AC switch	24 10/100 Ethernet ports, 2 1000X standard SFP <sup>1</sup> module slots, 2 1000X ES <sup>2</sup> SFP slots, and field-replaceable AC power supply	Cisco IOS Release 12.1(14)AX
Catalyst 3750 Metro 24-DC switch	24 10/100 Ethernet ports, 2 1000X standard SFP module slots, 2 1000X ES SFP slots, and field-replaceable DC power supply	Cisco IOS Release 12.1(14)AX
SFP modules	1000BASE-T, 1000BASE-SX, and 1000BASE-LX 1000BASE-ZX and CWDM <sup>3</sup> DWDM <sup>4</sup> and 100BASE-FX MMF <sup>5</sup>	Cisco IOS Release 12.1(14)AX Cisco IOS Release 12.1(14)AX1 Cisco IOS Release 12.2(25)EY

1. SFP = small form-factor pluggable
2. ES = enhanced services
3. CWDM = coarse wavelength-division multiplexer
4. DWDM = dense wavelength division multiplexing
5. MMF = multimode fiber

# Uploading the Switch Software

These are the procedures for downloading software:

- “Finding the Software Version and Feature Set” section on page 3
- “Deciding Which Files to Use” section on page 3
- “Upgrading a Switch by Using the CLI” section on page 4
- “Recovering from a Software Failure” section on page 5



**Note**

Before downloading software, read this section for important information.

## 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. 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.

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 the Cisco IOS image file. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 2 lists the software filename for this software release.

**Table 2 Cisco IOS Software Image Files for Catalyst 3750 Metro Switches**

Filename	Description
3750me-i5-tar.122-25.EY4.tar	Cisco IOS image tar file. This image has Layer 2+ and Layer 3 features.
c3750me-i5k2-tar.122-25.EY4.tar	Cisco IOS cryptographic image tar file. This image has the Kerberos, SSH <sup>1</sup> , SSL <sup>2</sup> , Layer 2+, and Layer 3 features.

1. SSH = Secure Shell
2. SSL = Secure Socket Layer

## Upgrading a Switch by Using the CLI

This procedure is for copying the 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.

Download the software from Cisco.com to your management station by following these steps:

---

**Step 1** Use [Table 2 on page 3](#) to identify the file that you want to download.

**Step 2** Download the software image file from Cisco.com.

Go to this URL and log in to download the appropriate files:

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

To download the files, click the link for your switch platform, and then follow the links on the page to select the correct tar image file.

**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, see Appendix B in the software configuration guide for this release.

**Step 4** Log in to the switch through the console port or a Telnet session.

**Step 5** Check your VLAN 1 configuration by using the **show interfaces vlan 1** privileged EXEC command, and verify that VLAN 1 is part of the same network as the TFTP server. (Check the *Internet address is* line near the top of the display.)

**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 using 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 been 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/c3750me-i5-tar.122-25.EY.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

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity. You can use the Xmodem protocol to recover from these failures.

For detailed 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 (See the *Catalyst 3750 Metro Switch Hardware Installation Guide*.)
- The CLI-based setup program (See the *Catalyst 3750 Metro Switch Hardware Installation Guide*.)
- The DHCP-based autoconfiguration (See the *Catalyst 3750 Metro Switch Software Configuration Guide*.)
- Manually assigning an IP address (See the *Catalyst 3750 Metro Switch Software Configuration Guide*.)

## New Features

These are the new supported hardware and the new software features provided this release:

- [“New Hardware Features” section on page 5](#)
- [“New Software Features” section on page 5](#)

## New Hardware Features

For a list of all supported hardware, see the [“Hardware Supported” section on page 2](#).

## New Software Features

This release has no new software features.

# Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release required to support the major features on the Catalyst 3750 Metro switch.


**Note**

Features not included in the table are available in all releases. You can see a list of features from the first release at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750m/12225ey/3750msgc/swintro.htm>

**Table 3** Catalyst 3750 Metro Switch Features and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
IEEE 802.1x accounting and MIBs (IEEE8021-PAE-MIB and CISCO-PAE-MIB)	12.2(25)EY
DHCP snooping with the option-82 information option	12.2(25)EY
DHCP snooping binding database configuration	12.2(25)EY
Dynamic ARP inspection	12.2(25)EY
EtherChannel guard	12.2(25)EY
Flex Links	12.2(25)EY
IGMPv3 snooping	12.2(25)EY
IGMP throttling	12.2(25)EY
IP source guard	12.2(25)EY
MultipleVPN Routing/Forwarding (Multi-VRF) CE,	12.2(25)EY
Private VLAN	12.2(25)EY
SFP diagnostic management interface	12.2(25)EY
SSHv2 server application (cryptographic images only)	12.2(25)EY
SSL Version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)EY
Smartports macros	12.2(25)EY
Auto-QoS	12.2(25)EY
VLAN-based QoS and dual-level hierarchical policy maps on SVIs	12.2(25)EY
Matching the CoS of the inner tag for 802.1Q tunneling traffic.	12.2(25)EY
Applying hierarchical service policies in the inbound direction on an ES port.	12.2(25)EY
Storm control enhancements	12.2(25)EY
SFP diagnostic management interface	12.2(25)EY
Unicast MAC address filtering	12.2(25)EY
QoS egress priority queue	12.1(14)AX2
QoS DSCP transparency	12.1(14)AX2
Point-to-point Layer 2 protocol tunneling	12.1(14)AX1

# 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.

- [“Configuration” section on page 7](#)
- [“Ethernet” section on page 9](#)
- [“Fallback Bridging” section on page 9](#)
- [“HSRP” section on page 9](#)
- [“IP” section on page 9](#)
- [“IP Telephony” section on page 10](#)
- [“Multicasting” section on page 10](#)
- [“MPLS and EoMPLS” section on page 10](#)
- [“Multicasting” section on page 10](#)
- [“QoS” section on page 12](#)
- [“Routing” section on page 13](#)
- [“SPAN and RSPAN” section on page 13](#)
- [“Trunking” section on page 14](#)
- [“Tunneling” section on page 14](#)
- [“VLAN” section on page 14](#)

## 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)
- 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 12.2(25)EY. (CSCec35100)

- 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:
  - 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.
  - 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.
  - 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)

- 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)
- 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)
- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered for 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 for that specific interface. (CSCee93822)
- The Catalyst 3750 Metro switch does not learn its own MAC address on Layer 2 interfaces. For example: Ports 1/0/1 and 1/0/2 belong to VLAN x, port 1/0/3 is a Layer 3 port with an IP address that belongs to the subnet of VLAN x, and ports 1/0/2 and 1/0/3 are connected. In this case, a host connected to port 1/0/1 cannot ping port 1/0/3. The switch does not update the CAM table and does not use the MAC address of port 1/0/3 in the CAM table for port 1/0/2.

The workaround is to statically configure the MAC address of port 1/0/3 in the CAM table of the switch bound to port 1/0/2 by using the **mac address-table static mac-addr vlan vlan-id interface fastethernet1/0/2** global configuration command. (CSCee87864)

- 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

This is the Ethernet limitation:

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)

## Fallback Bridging

These are the fallback bridging limitations:

- If a bridge group contains a VLAN that has a static MAC address 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 under this condition: 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. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group bridge-group** interface configuration command. Another workaround is to disable port security on all ports in all VLANs participating in fallback bridging by using 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:

- The switch does not create an adjacency table entry when the Address Resolution Protocol (ARP) timeout value is 15 seconds and the ARP request times out.

The workaround is to set an ARP timeout value higher 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 an 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 VVID relearns the IP phone MAC address. MAC addresses are deleted manually or automatically for a topology change or when port security or an IEEE 802.1x feature is enabled or disabled. There is no workaround. (CSCea80105)
- After changing the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x capable ports, it takes approximately 30 seconds before the address is relearned. There is no workaround. (CSCea85312)

## 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)

## MPLS and EoMPLS

These are the multiprotocol label switching (MPLS) and Ethernet over MPLS (EoMPLS) limitations:

- Port-based Ethernet over Multiprotocol Label Switching (EoMPLS) sessions do not function if the incoming port is configured as an Inter-Switch Link (ISL) trunk. The workaround is to configure the incoming ports as an 802.1Q trunk or as an access port. (CSCeb44014)
- The display for the **show mpls ldp neighbor ipaddr-of-neighbor detail** user EXEC command always shows the targeted hello holdtime value as *infinite*. The workaround is to use the **show mpls ldp parameter** user EXEC command to see the configured value. (CSCeb76775)
- When MPLS is enabled, traceroute is not supported. There is no workaround. (CSCec13655)

## Multicasting

These are the multicasting limitations:

- 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.

- 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 VLAN group, but it is a member in some other VLAN group. Unnecessary traffic is sent on the trunk port and needlessly reduces the bandwidth of the port. There is no workaround 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)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number in the Switch Database Management (SDM) template shown with 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)
- 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 access to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL configured 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 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)
- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable and then re-enable IP multicast routing on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.
 The workaround is to enter **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

## QoS

These are the 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 ten to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When traffic with different class of service (CoS) values is sent into a 802.1Q tunnel, only the CoS 0 statistics increment in the **show mls qos interface** user EXEC command display. There is no workaround. (CSCeb75230)
- The **bandwidth** interface configuration command is not supported at the interface level, but it appears in the CLI. There is no workaround. (CSCeb80223)
- The **random-detect** interface configuration command is not supported at the interface level, but it appears in the CLI. There is no workaround. (CSCeb80300)
- The display for the **show policy-map interface** user EXEC command shows zeros for the counters associated with class-map match criteria. There is no workaround. (CSCec08205)
- The **priority** policy-map class configuration command cannot be configured for the default traffic class in a policy map. The workaround is to configure explicit matches for traffic that requires priority treatment. (CSCec38901)
- Modifying a QoS class within a very large service policy that is attached to an ES port can cause high CPU utilization and an unresponsive CLI for an excessive period of time. The workaround is to detach the service policy from the port while making the modifications and then to re-attach the service policy. (CSCec75945)
- When packets are queued for egress on an ES port due to the application of a QoS service policy, they consume packet buffer memory on the switch. If many queues are simultaneously congested and are unable to drain, packet loss can occur in either direction (ingress or egress) due to the lack of buffer memory. If this becomes a problem, you can change switch behavior by using the **queue-limit** policy-map class configuration command at the class level to set shorter queue depths. Each shaper has an associated buffer queue with a default depth of 128 packets.

For example:

```
Switch(config)# policy-map cos2-policy
Switch(config-pmap)# class cos2
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# queue-limit 32
```

The point at which buffer memory is exhausted depends on the number of queues, the sizes of the queued packets, and whether or not the traffic pattern being sent to the switch allows the queues to drain at all.

Upgrading your switch to Cisco IOS Release 12.2(25)EY greatly reduces the possibility of this situation happening, although it can still occur with some configurations and traffic patterns. (CSCed83886)

- 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:

- 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.
- A route map that contains an ACL with a DSCP clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and issues an error message that shows that the route map is unsupported. There is no workaround. (CSCea52915)
- 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. There is no workaround for a remote SPAN session. 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)
- During periods of very high traffic and 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 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 at 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, this 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)

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

## Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the port 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).

## Tunneling

This is the tunneling limitation:

- VLAN mappings can be configured on a per-interface basis. A different set of mappings can be configured on each ES interface. The per-interface VLAN mappings remain in effect even when the ES ports are bundled in an EtherChannel. For example, if you map Gigabit Ethernet 1/1/1 to VLAN 20 through VLAN 50 and Gigabit Ethernet 1/1/2 to VLAN 20 through VLAN 70, traffic on VLAN 20 leaving the switch through the ES port bundle should be load balanced across the individual ES interfaces. However, some of that traffic is incorrectly translated to VLAN 50, and some is incorrectly translated to VLAN 70. The workaround is to configure identical VLAN mappings on both ES ports if they are going to be bundled into an EtherChannel. (CSCec49520)

## VLAN

These are the VLAN limitations:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13000, the switch can halt. The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- 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

- When you apply a per-VLAN QoS per-port policer policy-map to a VLAN 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)

## Important Notes

These are the important notes related to this software release:

- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(25)EY and later. In software releases earlier than Cisco IOS Release 12.2(25)EY, 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)

- Beginning with Cisco IOS Release 12.2(25)EY, ISL encapsulation is supported only on standard ports and not on enhanced services (ES) ports. The ES ports support only 802.1Q encapsulation and the **switchport trunk encapsulation** interface configuration command is no longer visible on these ports. When you are upgrading a switch from Cisco IOS Release 12.1(14)AX to Cisco IOS Release 12.2(25)EY or later, during the initial configuration process, the switchport trunk encapsulation option is rejected on ES ports and an error message appears. You can ignore this error message. If you save the new configuration by using the **copy running-config startup-config** privileged EXEC command and later re-install the Cisco IOS Release 12.1(14)AX image, the trunk encapsulation method originally configured on ES ports is lost and the ES ports use the default encapsulation method, which is to negotiate.
- In Cisco IOS Release 12.1(14)AX and earlier, port-based EoMPLS sessions could only be configured on switch ports. In Cisco IOS Release 12.2(25)EY and later, port-based EoMPLS sessions can only be configured on routed ports.




---

**Note** This change is handled automatically during an upgrade to Cisco IOS 12.2(25)EY or later, but if a configuration is written to NVRAM and the switch is then reloaded with Cisco IOS 12.1(14)AX, the new-style configuration is lost.

---

- Beginning with Cisco IOS Release 12.2(25)EY, you must specify the encapsulation type when using the **xconnect** interface configuration command.




---

**Note** This change is handled automatically during an upgrade to Cisco IOS 12.2(25)EY or later, but if a configuration is written to NVRAM and the switch is then reloaded with Cisco IOS 12.1(14)AX, the new-style configuration is lost.

---

- In Cisco IOS Release 12.1(14)AX1, the switch supported point-to-point Layer 2 protocol tunneling, which was not documented in the Cisco IOS Release 12.1(14)AX software documentation. This information is in the *Release Notes for the Catalyst 3750 Metro Switch, Cisco IOS Release 12.1(14)AX1* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750m/12114ax/ol464602.htm#wp44273>

This information is part of Chapter 26, “Configuring QoS.” For the complete chapter (minus these updates), go to this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750m/12114ax/3750msg/swqos.htm>

## Open Caveats

These are the Cisco IOS severity-3 open configuration caveats with possible unexpected activity in this software release:

- CSCeb35422

On a voice VLAN port with both IEEE 802.1x and port security enabled, dynamic secure addresses might not get deleted when the port is changed from multihost mode to single-host mode. This means that addresses learned in the multihost mode are still allowed after changing to single-host mode. This problem occurs under these conditions:

- The port is in an authorized state.
- The port learns the MAC addresses of multiple hosts.
- VLAN assignment is not enabled for the authorized host.

The workaround is to disable and then re-enable port security on the port.

- CSCeb42929

The switch does not work with the User Registration Tool (URT). The PC attempting to connect to the network can login successfully, but 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.

- CSCec19825

When the receive rate is 100 Mbps and the sample interval (historyControlInterval) is more than 45 seconds, the calculation of the SNMP etherHistoryUtilization report is incorrect and shows a much lower utilization than expected. This also occurs at lower receive rates if the interval is long.

The workaround is to set the historyControlInterval to less than 30 seconds. Longer intervals can cause the counters to overflow if the traffic is intense.

- CSCef37624

You cannot ping a Layer 3 interface that has a Network Address Translation (NAT) configuration.

There is no workaround.

- CSCef65928

When a class map of an attached policy map has its match condition removed and is then re-applied, some free memory is lost.

The workaround is to remove the class map from the policy map and then modify the match condition.

- CSCef67261  
When more multicast groups are configured than are supported by the currently-selected Security Device Manager (SDM) template, layer two multicast traffic is flooded on one or more multicast groups.  
There is no workaround.
- CSCef94884  
Unconfiguring OSPFv3 causes a memory leak.  
There is no workaround.
- CSCeg27382  
If the per-VLAN QoS per-port policer policy-map is already attached to a VLAN Switched Virtual Interface (SVI), do not modify the second level (port-level) policy-map. If you modify the policy-map by removing the policer while it is still attached, an error message appears, and the policy-map is detached by the switch. The policer cannot be re-applied back to that policy-map.  
The workaround is to redefine the second-level (port level) policy map if the policy map has already been detached by the system.
- CSCeg29704  
When QoS is enabled, bursty and TCP-based applications might have significant performance degradation due to unexpected packet drops on some of the egress queues.  
The workaround is to tune the egress queue buffer allocation and bandwidth scheduling parameters to allocate more bandwidth and buffer space to the affected queues.
- CSCeg52581  
If you start a session on a switch cluster member by using the **rcommand** user EXEC command, the commands that you enter in the rcommand session are always allowed, irrespective of the authorization status.  
There is no workaround.
- CSCeg77479  
If the pathnames for the system image and boot filenames are more than 75 characters each, only the first 75 characters are displayed when you enter the **show version** user EXEC command.




---

**Note** This does not affect the functionality of the switch.

---

The workaround is to enter the dir flash: user EXEC to view the names of the image files on the switch. The output of the command displays the image name of the file that will boot the *next* time the switch is loaded. It might be different from the current running image.

- CSCeh15382  
When a customer-edge (CE) device is connected to a Catalyst 3750M switch through an EtherChannel that is in an Ethernet over MPLS (EoMPLS) port tunnel, reloading the CE can cause a traceback error similar to the following in the PE device at the other end of the tunnel (if that device is also a Catalyst 3750M switch).  

```
02:20:31: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: Class ADJ: - unable to
unprovision segment 1. -Traceback= 252620 F195C8 11C80BC F19B04 F16A8C F16B28 F18AD0
F18D7C 33DF68 3381AC
```

  
There is no workaround. The system recovers automatically.

- CSCeh20081

When a trunk interface is converted to an IEEE 802.1Q tunnel, a traceback error similar to the following might appear:

```
3d20h: %PLATFORM_UCAST-3-LB: PI<->PD handles out of sync for Adj 222.1.1.1 Lb
-Traceback= 252620 A9204C A84E60 A86260 A92E7C AA36A0 AA3520 A96C60 A8A288 A78DC4
B095C8
```

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

- CSCeg76540

Hot Standby Routing Protocol (HSRP) does not function on multiprotocol label switching (MPLS) interfaces.

There is no workaround. Do not configure HSRP on MPLS interfaces.

- CSCeh12034

A Catalyst 3750M compares incoming MPLS traffic against the MPLS maximum transmission unit (MTU) size and drops traffic that violates the MTU size. The switch also correctly applies the MTU-size check on outgoing traffic.

There is no workaround. This is only an issue if the incoming MPLS MTU size is greater than the Catalyst 3750M MPLS MTU size.

- CSCeh25207

If a hierarchical service policy attached to an enhanced services (ES) interface is modified to include an invalid statement (for example, a *set* action in a VLAN class or a mixture of VLAN and QoS class matches at the same level of the hierarchy), error messages appear, but the switch does not automatically roll back to the last valid configuration.

If the error messages are ignored and QoS is globally disabled and re-enabled, the switch reloads.

If a service-policy modification causes in an error message to appear, the workaround is to manually remove the invalid statement by using the **no** form of the configuration option. The invalid configuration should never be written to NVRAM.

- CSCeh16771

In a hierarchical service policy, if a two-rate, three-level policer does not have a specified action to perform on packets that exceed the peak information rate (PIR), the switch configuration might contain corrupted characters instead of the action when the configuration is written to NVRAM. If the switch is then reloaded, the policer is rejected because of the corrupted configuration.

The workaround is to specify the action to perform on packets that exceed the PIR in the two-rate, three-level policer.

- CSCeh21255

When Ethernet over MPLS (EoMPLS) is configured on a switch, if one ES port is put in an EtherChannel and the other ES port is left as a trunk, a Layer 2 loop can be generated, and a CPUHOG traceback can appear if looped traffic is being process by the CPU.

The workaround is to remove the ES port from the EtherChannel. To avoid the condition when breaking up an EtherChannel that consists of ES ports, remove the port-channel interface, or remove the interfaces from the port-channel simultaneously by using the **interface range** configuration option.

- CSCeh13477

When ES interfaces in an EtherChannel are carrying Multiprotocol Label Switching (MPLS) traffic and more routes are configured than are supported in the SDM template, messages similar to the following might appear when the interface is shut down and brought back up:

```
2d20h: %PLATFORM_UCAST-3-LB: PI<->PD handles out of sync for Adj 222.1.1.1 LB
-Traceback= 252620 A919CC A847E0 A85BE0 A927FC AA2D28 A965E0 A89C08 A78744 B08F48
ADF504 ADDC4C AE3460 AD25CC B94AA0 B94F20
```

There is no workaround.

## Resolved Caveats

These are the caveats that have been resolved in these releases.

- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EY4” section on page 19](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EY3” section on page 20](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EY2” section on page 20](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EY1” section on page 22](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EY” section on page 22](#)

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EY4

These caveats were resolved in Cisco IOS Release 12.2(25)EY4:

- CSCek26492

Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

- CSCek37177

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

This issue is documented as Cisco bug ID [CSCek37177](#).

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-20070124-crafted-tcp.shtml>

- CSCse08786

This DDTS documents changes in how IOS handles packets destined to the router or switch.

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EY3

These caveats were resolved in Cisco IOS Release 12.2(25)EY3:

- CSCei61732

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

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

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

- CSCei76358

Through normal software maintenance processes, Cisco is removing deprecated functionality. These changes have no impact on system operation or feature availability.

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EY2

These caveats were resolved in Cisco IOS Release 12.2(25)EY2:

- CSCee45312

Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected.

Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

Refer to the Security Advisory at the following URL for more details

<http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>

- CSCeh11361
 

The switch no longer drops Routing Information Protocol version 1 (RIPv1) packets under these conditions:

  - The Border Gateway Protocol (BGP) is enabled on a switch interface, and the switch is configured as follows:
    - The **ip access-group** interface configuration command is not configured on the interface.
    - The **mac access-group** interface configuration command is not configured on the interface.
    - The **vlan access-map** global configuration command is not configured on the switch.
  - The Border Gateway Protocol (BGP) is enabled on a routed interface, and the **ip access-group** interface configuration command is not configured on the interface.
- CSCeh37667
 

IGMP packets are now forwarded through Ethernet over MPLS (EoMPLS) tunnels.
- CSCeh47274
 

A Catalyst 3750 Metro dual switch attached to the MPLS ring with Gigabit interfaces 1/1/1 and 1/1/2 does not receive traffic on EoMPLS tunnels if the incoming interface (Gigabit interface 1/1/1) is different from outgoing interface (Gigabit interface 1/1/2). This traffic interruption could happen because of asymmetric routing from one provider edge (PE) to another.
- CSCeh56495
 

The 3750 Metro no longer loses traffic when routing between VRF instances. If the switches are used as the provider edge customer-located equipment (PE-CLE) in customer sites, and both edges of the provider network are connected to customer premises equipment (CPE) switches, packets are no longer lost when switched between Virtual Private Network (VPN) routing and the Virtual Routing and Forwarding (VRF) process.
- CSCeh66692
 

Enabling an input policy on an enhanced-services (ES) interface no longer stops traffic.
- CSCeh80344
 

The upper range of a multi protocol label switching maximum transmission unit (MPLS MTU) is set with the system MTU command. When packets are received on a customer interface destined for tagged routes on MPLS interfaces, these packets are dropped for MPLS MTU violation. The upper range of MPLS MTU is limited by the system with the MTU jumbo setting.
- CSCeh82470
 

Hardware no longer fails to delete an old route if the next-hop changes. When an MPLS tagged route uses a recursive path that itself is not tagged, the hardware might not delete the route if the next hop changes. This scenario can cause packets to be forwarded on the old interface or be dropped.

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EY1

This caveat was resolved in Cisco IOS Release 12.2(25)EY1:

- CSCsa78000

When you enter the **show cdp neighbor detail** privileged EXEC command, your switch no longer restarts if it is one of these switches:

- Catalyst 3750, 3560, 3550, and 2970 switches running Cisco IOS Release 12.2(25)SEA or Cisco IOS Release 12.2(25)SEB
- Catalyst 3750 Metro switches running Cisco IOS Release 12.2(25)EY

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EY

These caveats were resolved in Cisco IOS Release 12.2(25)EY:

- 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 even after the group is deleted. MVR data traffic to the group stops flowing to the receiver port immediately stops after you enter the **no mvr group ip-address** global configuration command.

- CSCea90131

Under these conditions, the switch no longer reports a false security violation after an IEEE 802.1x supplicant is authenticated and assigned a new VLAN by the RADIUS server:

- IEEE 802.1x, port security, and voice VLAN are configured on a port.
- The maximum number of secure addresses has been learned on the port before it is authenticated.
- The VLAN assigned by the RADIUS server is different than the access VLAN configured on the port.
- The **show port-security** privileged EXEC command output no longer shows that the port is *SecureDown* when it is actually *SecureUp* and forwarding traffic correctly.

- CSCeb10032

The switch now passes Vine (Advanced Research Projects Agency) ARPA frames over bridge groups.

- CSCeb14406

DVMRP now correctly forwards packets.

- CSCeb29898

After starting up a switch 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.

- CSCeb54159

If an interface on the switch is mapped to queue-set 2, and you disable and then re-enable multilayer QoS globally by using the **mls qos** global configuration command, the interface is now mapped to the correct egress queue-set.

- CSCeb56226  
If an IEEE 802.1x port is configured for forced-unauthorized port control mode and voice VLAN, after you remove the voice VLAN and disable IEEE 802.1x on the port, the port now passes traffic.
- CSCec01607  
When you configure a policy-rate policer and attach it to an interface, the cdQosPoliceCfg table no longer shows two identical policers when only one has been configured. The cdQosPoliceStats table no longer contains status for two policers.
- CSCec13135  
The cbQosREDCfg, cbQosREDClassCfg and cbQosREDClassStats tables in CISCO-CLASS-BASED-QOS-MIB are now unsupported.
- CSCec57743  
The **no setup express** global configuration command now appears in the CLI Help menu when you enter the **no?** command.
- CSCec68807  
Memory allocation (malloc) and remote-procedure call (RPC) throttle messages no longer appear when one or more large access control lists (ACLs) are pasted to the console window.
- CSCec70857  
If you change the priority queue settings for ingress priority queue 2 by using the **mls qos srr-queue input priority-queue 2 bandwidth** global configuration command, the command is accepted correctly, and the configuration resulting from the **show running-config** privileged EXEC command no longer contains an extra **input**, for example, **mls qos srr-queue input priority-queue input 2 bandwidth**.
- CSCec72935  
The port bandwidth limit displayed by **show mls qos interface** user EXEC command is now correct and is no longer 100 minus the configured value.
- CSCec73580  
When the **switchport voice vlan {vlan-id | dot1p | none | untagged}** interface configuration command and the **spanning-tree bpduguard {disable | enable}** interface configuration command are configured together on an interface connected to another Catalyst 3750 Metro switch, the interface now becomes error-disabled when BPDUs are detected.
- CSCec84254  
On 10/100BASE-T interfaces, the switch now links up with some media converters running at 100 Mbps.
- CSCed12889  
When redundant uplinks are from the same stack member in a switch stack and UplinkFast is configured, dummy multicast packets are no longer sent.
- CSCed16780  
Layer 2 Protocol tunneling now functions reliably on EtherChannel interfaces.
- CSCed23767  
When you enter the **switchport port-security aging time** interface configuration command, the CLI Help no longer shows that entering 0 disables the aging time.

- CSCed29932  
When you change the Multiprotocol Label Switching (MPLS) router ID by entering the **mpls ldp router-id [loopback value] force** global configuration command, the local router ID is changed and the label distribution protocol (LDP) now binds with the LDP neighbor.
- CSCed30184  
An EtherChannel configured for 802.1Q tunneling and either the Port Aggregation Protocol (PAgP) or the Link Aggregation Control Protocol (LACP) does now come up.
- CSCed65285  
Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.  
  
Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)  
  
This advisory will be posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>
- CSCed65778  
Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.  
  
Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)  
  
This advisory will be posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>
- CSCed70488  
When an MPLS label is added to traffic leaving an enhanced services (ES) interface, any Layer 3 *set* operations (for rewriting the IP precedence or DSCP) that should apply to that traffic are now performed.
- CSCed82005  
If static IP source bindings are configured on an EtherChannel interface and the configuration is saved, the IP source bindings are no longer lost when the switch is reloaded.
- CSCed91730  
If Port Fast is enabled on the host ports and traffic is continuously received on that port, when a secondary VLAN is associated and then quickly disassociated, the MAC address tables across the switch stack no longer become unsynchronized.

- CSCed92268  
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 now programmed into the TCAM.
- CSCee07107  
ARP and reverse ARP (RARP) packets are now properly filtered by a configured VLAN map. In previous releases, if you enabled a VLAN for dynamic ARP inspection and a VLAN map was applied to the VLAN, ARP and RARP packets received in that VLAN on stack member ports were not dropped.
- CSCee08109  
An IEEE 802.1x per-user-based access control list (PUB-ACL) is now removed when an IEEE 802.1x client (for example, a PC) is disconnected from or disabled on a port.
- CSCee14018  
Port ACLs are now applied to IGMP control packets that have IP options.
- CSCee22721  
To make Intermediate System-to-Intermediate System (IS-IS) function on an SVI, you no longer need to manually set the Connectionless Network Service (CLNS) MTU to 1497.
- CSCee22376  
If an SNMP version 3 user is configured with the encrypted option and password, the switch no longer reloads when the MIB object usmUserAuthKeyChange is set.
- CSCee28016  
When IEEE 802.1x is enabled on a port and spanning-tree Port Fast is added to the interface configuration, the Port Fast configuration immediately appears. In previous releases, the configuration would sometimes not appear until a link up occurred, or the configuration would not appear on remote ports in a switch.
- CSCee29107  
If a switch has more than one route to reach a remote destination through an MPLS cloud, it now supports an EoMPLS configuration to that remote destination. This applies to both port-mode and VLAN-mode EoMPLS sessions.
- CSCee30284  
The EoMPLS tunneled ports (both port-based and VLAN-based) on a switch now tunnel Layer 2 protocol packets that are received from the customer switch to the remote (egress) provider edge switch.
- CSCee33525  
If you configure hundreds of QoS class maps, the switch no longer displays a `SYS-3-CPUHOG` message when you apply the service policy to an interface by using the **service-policy** interface configuration command or when you remove the service policy.
- CSCee37070  
When an IEEE 802.1x-enabled port is in single-host mode and has port security enabled, the port no longer goes into the error-disabled state and displays this system message if another MAC address is detected on the port:

```
%DOT1X-SECURITY_VIOLATION
```

- CSCee83209  
When the **default interface** *interface-id* interface configuration command is entered on a tunnel interface, the configuration is now completely cleared.
- CSCee87630  
When an enhanced services (ES) interface on a switch is configured as a Layer 2 switch port and MPLS is configured on a VLAN interface, you can now change the MPLS maximum transmission unit (MTU) on the VLAN interface.
- CSCee88546  
After a stack master failover, any per-user access control lists (ACLs) applied on authenticated IEEE 802.1x ports no longer appear twice when you enter the **show ip access-list** privileged EXEC command.
- CSCef10434  
When you set the duplex mode by using SNMP, the changes now appear in the output of the **show interface** *interface-id* | **include duplex** and the **show running interface** *interface-id* | **include duplex** commands.
- CSCef15273  
When you enable IEEE 802.1x accounting by using the **aaa accounting dot1x** global configuration command and an IEEE 802.1x port changes state, this traceback message no longer appears:  
%AAAA-3-TIMERNNOOPER:AAA/ACCT/TIMER: No periodic update but timer set.
- CSCef27079  
The **policy-map rename** global configuration command is not supported in Cisco IOS Release 12.2(25)EY.
- CSCef28173  
When you enter the **mls qos vlan-based** interface configuration command on an interface, the configuration that was previously configured by using the **mls qos cos override** interface is now correctly removed. The configuration remains removed even if you again enter the **no mls qos vlan-based** interface configuration command.
- CSCef37959  
The switch now generates an ARP request for the next policy-based routing (PBR) hop when it receives packets that should be policy routed.
- CSCef42632  
A per-VLAN Quality of Service (QoS) policy map that has a class map now works correctly if it is applied to a VLAN switched virtual interface (SVI) that uses an access control list (ACL) requiring Layer 4 port matching.
- CSCef58368  
You can now set the port speed to autonegotiate by using SMNP.
- CSCef60659  
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>.

- CSCef94585

The message `%SUPERVISOR-3-FATAL: MIC exception error 80` no longer appears under these conditions (in previous releases, all of these conditions had to occur for the message to appear):

- A per-VLAN QoS/per-port policer policy map is attached to two VLAN switched virtual interfaces (SVIs).
- The network has stacked switches.
- The policy map is detached and then reattached to one SVI interface.
- The policy map is detached from another SVI interface and then re-attached.

- CSCef65587

These error messages no longer randomly appear:

```
%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
```

- CSCeg27165

The switch no longer restarts when you enter the **auto qos voip cisco-phone** interface configuration command.

- CSCeg35590

If Cisco Express Forwarding (CEF) is disabled due to over-use of the switch content-addressable memory (CAM) resources, a subsequent BGP routing update no longer causes the switch to reload.

- CSCeg40067  
Both sides of a link no longer stay in the loop-inconsistent state under these conditions:
  - Rapid PVST is being used.
  - Loopguard is enabled, and there are multiple paths to the root bridge.
  - The root is either removed from the network or its priority changes.
- CSCeg46480  
A per-VLAN Quality of Service (QoS), per-port policy map that is attached to a VLAN Switched Virtual Interface (SVI) now works correctly on a port that has been changed from a switch port to router port and then back to a switch port again.
- CSCeg64282  
The port security MIB no longer issues a trap for a security violation for a port that is configured in the protect mode.
- CSCin68965  
A Cisco IP Phone no longer halts and displays the message *configuring IP* when two ports of the 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 phone is connected.

## Documentation Updates

This section provides these updates to the product documentation:

- [“Updates for the Software Configuration Guide” section on page 28](#)
- [“Updates for the Command Reference” section on page 29](#)
- [“Updates for the Hardware Installation Guide” section on page 29](#)

## Updates for the Software Configuration Guide

These are updates to the software configuration guide:

- In the “DHCP Snooping Binding Database” section in the “Configuring DHCP Features and IP Source Guard” chapter, the information in the third and fifth paragraphs is incorrect. This is the correct information:  
  
To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.  
  
When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. It also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.
- In the “Enabling the DHCP Snooping Binding Database Agent” section in the “Configuring DHCP Features and IP Source Guard” chapter, this information is added to Step 6:  
  
Use the **ip dhcp snooping binding** privileged EXEC command when you are testing or debugging the switch.

- In the “Enabling the DHCP Snooping Binding Database Agent” section in the “Configuring DHCP Features and IP Source Guard” chapter, the information about the **no ip dhcp snooping database** global configuration command is incorrect. This is the correct information:

To stop using the database agent and bindings file, use the **no ip dhcp snooping database** global configuration command.

- In the “Configuration Guidelines” section of the “Understanding Port Security” section in the “Configuring Port-Based Traffic Control” chapter, this information is incorrect:

Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.

This is the correct information:

Port security can only be configured on static access ports, trunk ports, or tunnel ports. A secure port cannot be a dynamic access port.

## Updates for the Command Reference

These are updates to the command reference:

- In Cisco IOS Release 12.2(25)EY1 and earlier, the range for the *message-interval-timer* in the **udld message time message-timer-interval** global configuration command is 7 to 90 seconds. In Cisco IOS Release 12.2(25)EY2 and later, the range for the *message-timer-interval* is 1 to 90 seconds.
- The description and usage guidelines for the **ip dhcp snooping database** global configuration command are incorrect. This is the correct information:
  - Use the **ip dhcp snooping database** global configuration command to configure the DHCP snooping binding database agent. Use the **no** form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.
  - If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Use the **no ip dhcp snooping database** command to disable the agent.

- In Cisco IOS Release 12.2(25)EY and later, the **snmp-server ifindex persist** global command is not supported.

## Updates for the Hardware Installation Guide

The Preface for the *Catalyst 3750 Metro Switch Hardware Installation Guide* does not include the translations for the Warning symbol and explanation (Statement 1071) or a change to the Warning statement about installation for short-circuit (overcurrent) protection (Statement 1005-Circuit Breaker) in Appendix E, “Translated Safety Warnings.”

This information is in the *Release Notes for the Catalyst 3750 Metro Switch, Cisco IOS Release 12.1(14)AX* at this URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750m/12114ax/ol464601.htm#35851>

## Related Documentation

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

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750m/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 30.

- *Catalyst 3750 Metro Switch Software Configuration Guide* (order number DOC-7816793=)
- *Catalyst 3750 Metro Switch Command Reference* (order number DOC-7816797=)
- *Catalyst 3750 Metro Switch System Message Guide* (order number DOC-7816792=)
- *Catalyst 3750 Metro Switch Hardware Installation Guide* (order number DOC-7815869=)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (not orderable but available on Cisco.com)

## 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)

### Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](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 Ordering tool:

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

- 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 1 800 553-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.

## Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

## Reporting Security Problems in Cisco Products

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

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

**Tip**

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

## 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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is 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/>

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

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

Copyright © 2005-2007 Cisco Systems, Inc. All rights reserved.