



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

Revised September 24

Cisco IOS Release 12.2(25)SEG and later run on the Catalyst 3750 Metro switch.

These release notes include important information about Cisco IOS Release 12.2(25)SEG and later 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 27.

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/prod_release_note09186a00801deec5.html#wp2367913



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

© 2006-2007 Cisco Systems, Inc. All rights reserved.

Contents

This information is in the release notes:

- [“Hardware Supported” section on page 2](#)
- [“Upgrading the Switch Software” section on page 3](#)
- [“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 8](#)
- [“Important Notes” section on page 17](#)
- [“Open Caveats” section on page 18](#)
- [“Resolved Caveats” section on page 20](#)
- [“Documentation Updates” section on page 23](#)
- [“Related Documentation” section on page 27](#)
- [“Obtaining Documentation” section on page 27](#)
- [“Obtaining Technical Assistance” section on page 30](#)
- [“Obtaining Additional Publications and Information” section on page 31](#)

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 ¹ module slots, 2 1000X ES ² 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 ³ 100BASE-FX MMF ⁴ 1000BASE-BX	Cisco IOS Release 12.1(14)AX Cisco IOS Release 12.1(14)AX1 Cisco IOS Release 12.2(25)EY Cisco IOS Release 12.2(25)EY2

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

Upgrading 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
- “Archiving Software Images” section on page 4
- “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
c3750me-i5-tar.122-25.SEG3.tar	Cisco IOS image tar file. This image has Layer 2+ and Layer 3 features.
c3750me-i5k91-tar.122-25.SEG3.tar	Cisco IOS cryptographic image tar file. This image has the Kerberos, SSH ¹ , SSL ² , Layer 2+, and Layer 3 features.

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

Archiving Software Images

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

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

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

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



Note

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

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html#wp1018426

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.SEG3.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 as described in the *Catalyst 3750 Metro Switch Getting Started Guide*.
- The CLI-based setup program as described in the *Catalyst 3750 Metro Switch Hardware Installation Guide*.
- The DHCP-based autoconfiguration as described in the *Catalyst 3750 Metro Switch Software Configuration Guide*.
- Manually assigning an IP addresses described in 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 6](#)
- [“New Software Features” section on page 6](#)

New Hardware Features

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

New Software Features

These are new software features for these releases:

- [New Software Features for Release 12.2\(25\)SEG1, page 6](#)
- [New Software Features for Release 12.2\(25\)SEG, page 6](#)

New Software Features for Release 12.2(25)SEG1

These are the new software features for this release:

- Optional configuration logger to log configuration changes made through the command-line interface (CLI), including the command that was used and who entered it. See the “[Configuration Change Logger](#)” section on page 23
- Enhanced support for Unique Device Identifier (UDI) feature. See the “[Unique Device Identifier \(UDI\) Enhancement](#)” section on page 25.

New Software Features for Release 12.2(25)SEG

These are the new software features for this release:

- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM) and Ethernet Local Management Interface (E-LMI).
- Nonstop forwarding (NSF) awareness to enable the Layer 3 switch to continue forwarding packets from an NSF-capable neighboring router during the interval when the primary route processor (RP) is failing and the backup RP is taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.
- Multiple spanning-tree (MST) based on the IEEE 802.1s standard.
- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files. Requires the cryptographic version of the software.
- Per-VLAN MAC address table learning disable.

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/en/US/products/hw/switches/ps5532/products_configuration_guide_chapter09186a00801ee872.html

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

Feature	Minimum Cisco IOS Release Required
CFM and E-LMI (Ethernet OAM)	12.2(25)SEG
NSF awareness	12.2(25)SEG
MST based on the IEEE 802.1s standard	12.2(25)SEG
SCP	12.2(25)SEG
Per VLAN MAC learning disable	12.2(25)SEG
DHCP Option-82 configurable remote Id and circuit ID	12.2(25)SEE
H-VPLS	12.2(25)SED
IEEE 802.1x restricted VLANs	12.2(25)SED
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 IEEE 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
Flex Link Preemptive Switchover	12.2(25)SEE
OSPF nonbroadcast and point-to-multipoint networks	12.2(25)SEE

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 8](#)
- [“Ethernet” section on page 10](#)
- [“Fallback Bridging” section on page 10](#)
- [“HSRP” section on page 10](#)
- [“IP” section on page 11](#)
- [“IP Telephony” section on page 11](#)
- [“MAC Addressing” section on page 11](#)
- [“MPLS and EoMPLS” section on page 11](#)
- [“Multicasting” section on page 12](#)
- [“QoS” section on page 13](#)
- [“Routing” section on page 14](#)
- [“SPAN and RSPAN” section on page 15](#)
- [“Trunking” section on page 16](#)
- [“Tunneling” section on page 16](#)
- [“VLAN” section on page 17](#)

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)

- On a switch running Cisco IOS Release 12.1(14)AX, when the **show interface** privileged EXEC is entered on a port that is running IEEE 802.1Q, inconsistent statistics from ports running IEEE 802.1Q might be reported.

The workaround is to upgrade to Cisco IOS Release 12.2(25)EY or later. (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)
- When enhanced services (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. (CSCeh13477)

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

These are the Hot Standby Routing Protocol (HSRP) limitations:

- 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)
- HSRP does not function on multiprotocol label switching (MPLS) interfaces.
There is no workaround. Do not configure HSRP on MPLS interfaces. (CSCeg76540)

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)

- 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 IEEE 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)

- When an ES port is configured as a trunk port and the switch is using VLAN-based EoMPLS, if the VLAN has been cleared from the trunks on the ES ports, packets destined to IP addresses 224.0.0.xxx might not be sent over the EoMPLS tunnel.

The workaround is to allow the EoMPLS VLAN on the trunk on the ES ports. (CSCsc42814)

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)
- When more multicast groups are configured than are supported by the selected Switch Database Management (SDM) template, Layer 2 multicast traffic is flooded on one or more multicast groups.
There is no workaround. (CSCef67261)

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 IEEE 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 or later 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 and does not apply to bridged packets.

The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. 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. 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 process egress-SPAN at up to 40,000 packets per second (64-byte packets). When the total traffic being monitored is below this limit, there is no degradation. However, if the traffic exceeds the limit, only a portion of the source stream is monitored. 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 monitored. If fallback bridging and multicast routing are disabled, egress-SPAN monitoring 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-span monitored. Packets that are susceptible to this problem are IGMP packets with 4 bytes of IP options (IP header length of 24). Examples of such packets are IGMP reports and queries having the router alert IP option. Ingress-span monitoring of such packets is not accurate and can vary with traffic rate. Typically, very few or none of these packets are monitored.

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 a local SPAN session. (CSCed24036)

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (IEEE 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 IEEE 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. This is 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 IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 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).

- When a trunk interface is converted to an IEEE 802.1Q tunnel, a traceback error message 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. (CSCeh20081)

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 13,000, 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 ES ports. The ES ports support only IEEE 802.1Q encapsulation and the **switchport trunk encapsulation** interface configuration command is no longer available 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 in this software release:

- CSCsd12172

If your switch is running Ethernet over multiprotocol label switching (EoMPLS) in Cisco IOS Release 12.2(25)SED, the service policy that is applied to the SVI might mark the traffic correctly but might police the traffic to a different value than the one defined in the service policy.

There is no workaround.

- CSCsd79916

When IEEE 802.1x authentication is configured on a voice VLAN port, the switch does not forward traffic if the attached PC is configured for both machine authentication and user authentication.

An authenticated 802.1X port might not forward traffic in these conditions:

- The port is assigned to a voice VLAN.
- The PC is configured for both machine authentication and user authentication.
- The machine-initiated and user-initiated authentications result in different VLANs being assigned to the port.

The workaround is to remove the voice VLAN configuration from the port or to configure the machine-authentication and user-authentication profiles to assign the same VLAN to the port.

- CSCsd87350

When you enter the **show policy-map interface *interface-id* input** privileged EXEC command, the service policy counters might not be correct. The counters might show a zero and not increment even when traffic is passing through the policy map on the interface.

The workaround is to enter the **no service-policy input *policy-map-name*** interface configuration command, followed by the **service-policy input *policy-map-name*** command to remove and reapply the service policy to the interface. The counter then should begin to work correctly.

- CSCsd97102

When you configure a hierarchical QoS service policy on an ES interface and then enter the **show policy-map interface** privileged EXEC command, the bridge protocol data units (BPDUs) shown in the output might be misclassified in a class with a Layer 3 match.

There is no workaround.

- CSCsd97378

When a non-hierarchical service policy is attached to an ES interface, traffic classes, including access-group matches, cannot be dynamically added to the service policy. An error message appears and the class cannot then be removed from the policy as long as it is attached to the interface.

The workaround is to first remove the policy map from the ES port by entering the **no service-policy input policy-map-name** interface configuration command. You can then modify the policy map traffic class and reattach it to the port.

- CSCse14774

If a switch is connected to a third-party router through an EtherChannel and the EtherChannel is running in Link Aggregation Control Protocol (LACP) mode, the interfaces in the EtherChannel might go down after you enter the **switchport trunk native vlan vlan-id** interface configuration command to change the native VLAN from VLAN 1 (the default) to a different VLAN ID.

These are the workarounds. You only need to do one of these:

- Do not change the native VLAN ID from the default setting of VLAN 1.
- If you need to change the native VLAN ID to a VLAN other than VLAN 1, do not run the EtherChannel in LACP mode, and change the mode to *On* by using the **channel-group channel-group-number mode on** interface configuration command.

- CSCse21219

If a Putty client is used to change the configuration to a device with SSH, the switch might stop responding to incoming traffic, such as SSH, Telnet, or ping packets. The switch responds to traffic after the TCP session is reset, which can take 7 minutes.

Use one of these workarounds:

- Use Putty Version 0.58.
- Enter a SSH, telnet, or ping command on the console.

- CSCse30660

When a hierarchical service policy is applied to a trunk interface, the way that the BPDUs are classified depends on whether or not the native VLAN on that trunk interface is explicitly added to the allowed VLAN list.

- If the native VLAN is not explicitly in the allowed VLAN list, the BPDUs match a class configured to match that VLAN.
- If the native VLAN is in the allowed VLAN list, the BPDUs are classified in the class default.

Resolved Caveats

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

- [Caveats Resolved in Cisco IOS Release 12.2\(25\)SEG3, page 20](#)
- [Caveats Resolved in Cisco IOS Release 12.2\(25\)SEG1, page 20](#)
- [Caveats Resolved in Cisco IOS Release 12.2\(25\)SEG, page 21](#)

Caveats Resolved in Cisco IOS Release 12.2(25)SEG3

These are the resolved caveats in Cisco IOS Release 12.2(25)SEG3:

- CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>.

- CSCsf04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmv3.shtml>

- CSCsj44081

Improvements have been made to User Datagram Protocol (UDP) processing.

Caveats Resolved in Cisco IOS Release 12.2(25)SEG1

These are the resolved caveats in Cisco IOS Release 12.2(25)SEG1:

- CSCef73145

The Mean Opinion Score (MOS) reported by an IP SLA jitter probe is now correct.

- CSCsb81283

MAC notifications now work properly when port security is configured.

- CSCsd26663
The switch no longer drops ICMPv6 router advertisements that are encapsulated in Ethernet frames with unicast or unknown destination addresses.
- CSCsd51530
When you telnet to a switch and enter the **autocommand-options nohangup** interface configuration command on VTY lines 0 through 4, you can now successfully log out and telnet back into the switch.

In previous releases, when you logged out of the switch and then tried to open a new Telnet session, the switch would automatically log you out.
- CSCse17494
When a switch is running Cisco Network Assistant and using TACACS+ for HTTPS (secure HTTP) authentication, the switch no longer fails if TACACS+ is not reachable.
- CSCse29173
Layer 2 multicast traffic is now forwarded by a switch after a port-channel link flap.
- CSCse39616
When port security is enabled, MAC addresses are now correctly relearned if a dynamic instance is present on the remote port.
- CSCse41647
The switch no longer reloads when interface flapping occurs and equal cost routes are present.

Caveats Resolved in Cisco IOS Release 12.2(25)SEG

These are the resolved caveats in Cisco IOS Release 12.2(25)SEG:

- 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>

- CSCea80105

When a Cisco IP Phone is connected to a switch, only the Voice VLAN (VVID) of the switch learns the MAC address of phone. This is the correct behavior.

In previous releases, the MAC address was learned on both the VVID and the Data VLAN (PVID). When the dynamic MAC addresses were removed (manually or automatically) either by a topology change or by enabling or disabling the port security or IEEE 802.1x feature, the MAC address of Cisco IP Phones MAC address was re-learned only on the VVID.
- CSCeg36369

A Catalyst ME 3750 switch now correctly learns the source MAC address of a Cisco Discovery Protocol (CDP) frame entering on a port that has CDP disabled.
- CSCei63394

When an IEEE 802.1x restricted VLAN is configured on a port and a hub with multiple devices is connected to that port, syslog messages are now generated because this is not a supported configuration. (Only one host should be connected to an IEEE 802.1x restricted VLAN port.)
- CSCei80087

It is no longer necessary to detach and then reapply a hierarchical policy map to force changes to a VLAN level class-map to take effect.
- CSCsb56438

There is no longer an extra index in the port table of the ciscoStpExtensions MIB that does not exist in the portCrossIndex MIB.
- CSCsb79198

A switch no longer fails IEEE 802.1x authentication if it downloads an access control list (ACL) that has more than 20 ACL access control entries (ACEs) from a RADIUS server.
- CSCsb82422

The switch now forwards an IEEE802.1x request that has *null* credentials.
- CSCsb97854

When a source port for a SPAN session has IEEE 802.1x enabled, Extensible Authentication Protocol over LAN (EAPOL) packets can now be seen by a packet-sniffing tool.
- CSCsc64095

The Intermediate System-to-Intermediate System (IS-IS) routing protocol now correctly establishes adjacencies when it is enabled on the VLAN 1 interface.
- CSCsc93768

The switch no longer fails when the VPN Routing and Forwarding (VRF) configuration is removed under these conditions:

 - VRF is removed by using the **no ip vrf** global configuration command.
 - Interfaces are configured in two or more VRFs.
 - One VRF has static address resolution protocols (ARPs) configured.
 - The VRF with static ARPs is removed first.

- CSCsd13962
The switch no longer might reload during startup when service policies are attached to non-ES interfaces.
- CSCsd43371
The Connectionless Network Service (CLNS) maximum transmission unit (MTU) on an interface is no longer incorrectly set to zero.
- CSCsd69347
Entering the **show sdm prefer dual-ipv4-and-ipv6 routing** privileged EXEC command, which is not supported on the Catalyst 3750 Metro switch, no longer might cause the switch to reload.
- CSCsd69967
If you enter the **no interface vlan *vlan-id*** global configuration command for a Layer 3 SVI that has inbound or outbound access lists attached to it, this no longer might cause the switch to reset.
- CSCsd75290
IS-IS now correctly establishes adjacencies on interfaces configured as IS-IS network point-to-point interfaces.
- CSCsd81153
The switch no longer might stop forwarding traffic following a Layer 2 forwarding path change that results in an update to the CAM table but no update to the hardware forwarding entry.

Documentation Updates

This section contains documentation updates.

- [Documentation Updates for Cisco IOS Release 12.2\(25\)SEG1, page 23](#)
- [Documentation Updates for Cisco IOS Release 12.2\(25\)SEG, page 26](#)

Documentation Updates for Cisco IOS Release 12.2(25)SEG1

These are the updates to documentation for this release:

- [Configuration Change Logger, page 23](#)
- [Unique Device Identifier \(UDI\) Enhancement, page 25](#)

Configuration Change Logger

Beginning with this release, you can enable a configuration logger to keep track of configuration changes made with the CLI. When you enter the **logging enable** configuration-change logger configuration command, the log records the session, the user, and the command that was entered to change the configuration. You can configure the size of the configuration log from 1 to 1000 entries (the default is 100). You can clear the log at any time by entering the **no logging enable** command followed by the **logging enable** command to disable and reenabling logging.

Use the **show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics} [provisioning]** privileged EXEC command to display the complete configuration log or the log for specified parameters.

The default is that configuration logging is disabled.

For information about the commands, see the *Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a8086.html#wp1114989

Beginning in privileged EXEC mode, follow these steps to enable configuration logging:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	archive	Enter archive configuration mode.
Step 3	log config	Enter configuration-change logger configuration mode.
Step 4	logging enable	Enable configuration change logging.
Step 5	logging size <i>entries</i>	(Optional) Configure the number of entries retained in the configuration log. The range is from 1 to 1000. The default is 100. Note When the configuration log is full, the oldest log entry is removed each time a new entry is entered.
Step 6	end	Return to privileged EXEC mode.
Step 7	show archive log config	Verify your entries by viewing the configuration log.

This example shows how to enable the configuration-change logger and to set the number of entries in the log to 500.

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end
```

This is an example of output for the configuration log:

```
Switch# show archive log config all
  idx  sess  user@line  Logged command
  38   11   unknown user@vty3  |no aaa authorization config-commands
  39   12   unknown user@vty3  |no aaa authorization network default group radius
  40   12   unknown user@vty3  |no aaa accounting dot1x default start-stop group
radius
  41   13   unknown user@vty3  |no aaa accounting system default
  42   14           temi@vty4  |interface GigabitEthernet4/0/1
  43   14           temi@vty4  | switchport mode trunk
  44   14           temi@vty4  | exit
  45   16           temi@vty5  |interface FastEthernet0/1
  46   16           temi@vty5  | switchport mode trunk
  47   16           temi@vty5  | exit
```

Unique Device Identifier (UDI) Enhancement

The **show inventory [raw]** user EXEC command allows you to display product identification (PID) information for all identifiable entities in the device. Beginning with this release, you can use the **show inventory *entity-name*** command to display a specific entity. The display shows the UDI, including PID, Version Identifier (VID), and Serial Number (SN) of that entity. See the [show inventory](#) command page that follows.

show inventory

Use the **show inventory** user EXEC command to display product identification (PID) information for the hardware.

```
show inventory [entity-name | raw] [ | {begin | exclude | include} expression]
```



Note

If you enter **show inventory ?** in the CLI help, the *entity-name* keyword does not appear in this release of the software, although it is supported and you can enter an entity name.

Syntax Description

<i>entity-name</i>	(Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet0/1) into which a small form-factor pluggable (SFP) module is installed.
raw	(Optional) Display every entity in the device.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEG	This command was introduced.

Usage Guidelines

The command is case sensitive. With no arguments, the **show inventory** command produces a compact dump of all identifiable entities that have a product identifier. The compact dump displays the entity location (slot identity), entity description, and the unique device identifier (UDI), including PID, Version Identifier (VID), and Serial Number (SN) of that entity.

If there is no PID, no output appears when you enter the **show inventory** command.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: "1", DESCR: "ME-C3750-24TE"
PID:           , VID:           , SN:

NAME: "GigabitEthernet1/1/2", DESCR: "1000BaseSX SFP"
PID:           , VID:           , SN: A50015093
```

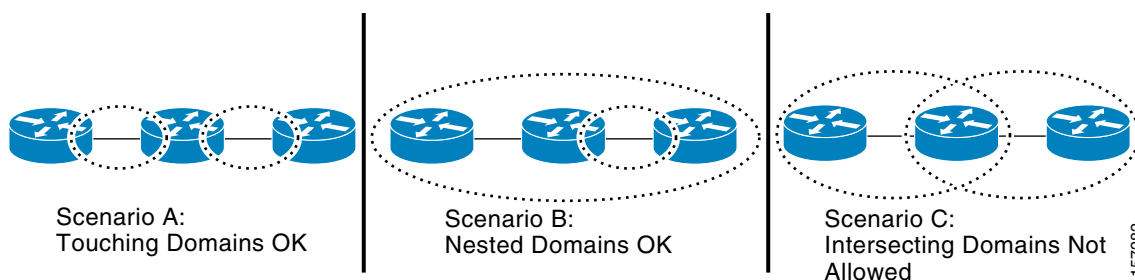
Documentation Updates for Cisco IOS Release 12.2(25)SEG

This section includes the updates to documentation for this release.

Correction to the Software Configuration Guide

In Chapter 36, “Configuring Ethernet CFM and E-LMI,” Figure 36-2 originally showed incorrect examples for Scenario B and Scenario C. The illustration has been corrected as shown below:

Figure 36-2 Allowed Domain Relationships



IP SLAs Support

The Catalyst 3750 Metro switch includes partial support for Cisco IOS IP Service Level Agreements (IP SLAs) to provide advanced network service monitoring information and collect data pertaining to SLAs verification. The switch can initiate and reply jitter probes. However, the traffic does not follow the queuing configuration that is applied to customer traffic. All locally originated traffic always goes to the same egress queue on the switch port, regardless of the ToS setting for the IP SLAs probe. We recommend the use of an external shadow router to measure latency and packet drop rate (PDR) across the switch.

For performance testing purposes, this configuration was validated:

1. Two switches connected back-to-back.
2. No protocols running on the switch CPUs, including STP.
3. Jitter probe send and receive rate:
 - a. 50 bidirectional probes sent with each probe consisting of up to 50 packets sent at 1-second intervals.
 - b. Probes started with a 1-second stagger between each probe.

For information about IP SLAs on Cisco routers, see this URL:

http://www.cisco.com/application/pdf/en/us/guest/products/ps6602/c1244/cdccont_0900aecd804fb392.pdf

Related Documentation

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

http://www.cisco.com/en/US/products/hw/switches/ps5532/tsd_products_support_series_home.html

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 27.

- *Catalyst 3750 Metro Switch Getting Started Guide* (order number DOC-7817431=)
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Metro Switch* (order number DOC-7817432=)
- *Catalyst 3750 Metro Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Metro Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750 Metro Switch System Message Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Metro Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (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/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

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

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:
http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm
- 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 rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

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

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

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

- Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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



Note

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

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

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

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

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

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

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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, 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, 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, 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. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006-2008 Cisco Systems, Inc. All rights reserved.