



Release Notes for the Catalyst 3750 Metro Switch Cisco IOS Release 12.2(40)SE

Revised January 6, 2009

Cisco IOS Release 12.2(40)SE runs on the Catalyst 3750 Metro switch.

These release notes include important information about Cisco IOS Release 12.2(40)SE 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 28.

You can download the switch software from this site:

<http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches>

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.

Contents

This information is in the release notes:

- “[Hardware Supported](#)” section on page 2
- “[Upgrading the Switch Software](#)” section on page 2
- “[Installation Notes](#)” section on page 5
- “[New Features](#)” section on page 5
- “[Minimum Cisco IOS Release for Major Features](#)” section on page 6



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

© 2007–2009 Cisco Systems, Inc. All rights reserved.

- [“Limitations and Restrictions” section on page 8](#)
- [“Important Notes” section on page 17](#)
- [“Open Caveats” section on page 18](#)
- [“Resolved Caveats” section on page 22](#)
- [“Documentation Updates” section on page 23](#)
- [“Related Documentation” section on page 28](#)
- [“Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page 29](#)

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	Cisco IOS Release 12.1(14)AX
	1000BASE-ZX and CWDM ³	Cisco IOS Release 12.1(14)AX1
	100BASE-FX MMF ⁴	Cisco IOS Release 12.2(25)EY
	1000BASE-BX	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 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
c3750me-i5-tar.122-40.SE.tar	Cisco IOS image tar file. This image has Layer 2+ and Layer 3 features.
c3750me-i5k91-tar.122-40.SE.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.122-37.SE1.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 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

These are the new software features for this release:

- Multicast Listener Discovery (MLD) snooping to enable distribution of IP version 6 (IPv6) multicast data to clients and routers in a switched network (Catalyst 2960 switches)
- IPv6 host support for basic IPv6 management of the Catalyst 2960 switch (Catalyst 2960 switches)
- Support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6, an enhanced version of IGRP. It utilizes IPv6 transport, communicates with IPv6 peers, and advertises IPv6 routes
- Private VLANs to allow traffic to be segmented at the data-link layer (Layer 2) OSI model, limiting the size of the broadcast domain. This enables a greater number of VLANs and reduces the number of unused subnet addresses.

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
Configuration replacement and rollback	12.2(40)SE
Embedded event manager (EEM)	12.2(40)SE
Internet Group Management Protocol (IGMP) Helper	12.2(40)SE
IP Service Level Agreements (IP SLAs) support	12.2(40)SE
IP SLAs EOT	12.2(40)SE
IP SLAs for Metro Ethernet using IEEE 802.1ag Ethernet operation, administration, and maintenance (OAM)	12.2(40)SE
Multiprotocol label-switching (MPLS) OAM	12.2(40)SE
Multicast virtual routing and forwarding (VRF) lite	12.2(40)SE
Support for the SSM PIM protocol	12.2(40)SE
Support for the Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE
Support for Resilient Ethernet Protocol (REP)	12.2(40)SE
Ethernet OAM MPLS	12.2(37)SE
ELMI-CE	12.2(37)SE
LLDP and LLDP-MED	12.2(37)SE
Port security on a PVLAN host	12.2(37)SE
VLAN Flex Links load balancing	12.2(37)SE
MVR over trunk port (MVRoT) support	12.2(35)SE1
Hierarchical QoS on ES EtherChannels	12.2(35)SE1
Enhanced object tracking for HSRP	12.2(35)SE1
Ethernet OAM IEEE 802.3ah protocol	12.2(35)SE1
Ethernet OAM CFM (IEEE 802.1ag) and E-LMI	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

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

Feature	Minimum Cisco IOS Release Required
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](#)
- [“logging event-spanning-tree Command” section on page 13](#)
- [“QoS” section on page 13](#)
- [“Routing” section on page 15](#)
- [“SPAN and RSPAN” section on page 15](#)
- [“Trunking” section on page 16](#)
- [“Tunneling” section on page 17](#)
- [“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 enhanced-services (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)

logging event-spanning-tree Command

When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

Use one of these workarounds:

- Disable logging to the console.
- Rate-limit logging messages to the console. (CSCsg91027)
- Remove the **logging event spanning-tree** interface configuration command from the interfaces.
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

The workaround is to configure aggressive UDLD. (CSCsh70244).

QoS

These are the Quality of Service (QoS) limitations:

- For MPLS VPN, you cannot use the enhanced-services (ES) port QoS to perform per-VRF QoS because the network processor cannot identify VRFs. You can use standard QoS on a non-ES port to perform upstream traffic rate limiting by using hierarchical QoS policers applied at the SVI. You cannot use this method for downstream traffic rate limiting because the switch does not support applying egress policers to an SVI.
- 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 enhanced-services (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 enhanced-services (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 an enhanced-services (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 notes apply to Cisco IOS software:

- Cisco IOS Release 12.2(40)SE and later

If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software to Cisco IOS Release 12.2(40)SE (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

```
AutoQoS Error: ciscophone input service policy was not properly applied
policy map AutoQoS-Police-CiscoPhone not configured
```

If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

- 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 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.

Open Caveats

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

- CSCsh04718

When you try to apply a service policy to an interface, you might see this error message:

```
QoS: Error setting QinQ policy, error in allocating NP memory
QoS: Failed to upload service policy for port Gi1/1/2 Service Policy attachment
failed.
```

This can occur when the allowed number of match records is exceeded.

The workaround, if you see this error, is to not use a match statement in an IEEE 802.1Q tunneling class-map in the policy-map that would result in more than 4096 tunneling match records for the tunneling pair.

- CSCsh12472

The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

```
15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
(ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
4CEB50 859DF4 A7BF28 A98260 882658 879A58
```

There is no workaround.

- CSCsh36186

When using Enhanced IGRP (EIGRP), a route might not appear in the routing table after booting up or during link flap.

The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command on the affected interface.

- CSCsi01526

Traceback messages appear if you enter the **no switchport** interface configuration command to change a Layer 2 interface that belongs to a port channel to a routed port.

There is no workaround.

- CSCsi06399

When a RIP network and IP address are configured on an interface, a traceback error occurs after you enter the **shutdown**, **no shutdown**, **switchport** and **no switchport** interface configuration commands.

The workaround is to configure the RIP network and the IP address after you configure the interface.

- CSCsi32590

When Cisco Discovery Protocol (CDP) is enabled on a dot1q tunnel interface and a shutdown and then no shutdown are issued on the link, CDP is no longer enabled.

There is no workaround.

- CSCsi44924

On a Catalyst 3750 Metro switch running Cisco IOS release 12.2(35)SE2 or later, if you attach or modify a policy with a policer action that has a user-configured conform burst (bc) or peak burst (be) specified in milliseconds by using the **police cir percent percent [bc conform-burst ms] | pir percent percent [be peak-burst ms]** policy map configuration command, you might receive a false error message related to *adjusting bc/be value to fit the interface supported range*.

The workaround is to use the **police cir cir** policy-map class configuration command and to specify the committed information rate (CIR) as an absolute number in bits per second (b/s) instead of a percentage.

- CSCsi46093

When an internal VLAN is configured as a preferred VLAN for Flex Link VLAN load-balancing ports, traffic loss might occur on the internal VLAN.

The workaround is to remove the interval VLAN from the Flex Link VLAN load-balancing preferred VLAN lists for both the active and backup interfaces.

- CSCsi63999

Changing the spanning tree mode from rapid STP to MSTP can cause tracebacks when the virtual port error-disable feature is enabled when the STP mode is changed.

There is no workaround.

- CSCsi70454

The configuration file used for the configuration replacement feature requires the character string *endn* at the end of the file. The Windows Notepad text editor does not add the *endn* string, and the configuration rollback does not work.

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

- Do not use a configuration file that is stored by or edited with Windows Notepad.
- Manually add the character string *endn* to the end of the file.

- CSCsj10198

When a per-port per-VLAN policy map (a hierarchical VLAN-based policy map) is attached to a VLAN interface, and you remove the child-policy policer from the policy map and then add it back, the policy map fails to re-attach to the same SVI

The workaround is to delete the child policy, which removes it from the parent policy. Then recreate the child policy (with the same or a different name) and reference it in the parent policy. The parent policy then successfully attaches to the SVI.

- CSCsj21718

When system jumbo MTU size is configured on a switch and the egress ports can support jumbo frames, the egress SPAN jumbo frames are not forwarded to the SPAN destination ports. In a mixed hardware stack of Catalyst 3750-E and 3750 switches, this problem occurs if the egress port is a switch port on a Catalyst 3750 switch.

There is no workaround.

- CSCsj22678

A delay can occur you remove an access control list (ACL) from a switch stack under these conditions:

- A QoS, per-port policy map is attached to a large number of switched virtual interfaces (SVIs) in the stack.
- A per-VLAN QoS, per-port policer policy map is attached to a large number of switched virtual interfaces (SVIs) in the stack
- The ACL to be removed is being used by the policy map.
- There are three or more switches in the stack.

The delay can increase, up to 30 minutes, depending on the number of SVIs that are attached to the policy map. The delay does not affect the operation of the policy-map. However, either of these workarounds will reduce the length of the delay:

- Remove the access control entries (ACEs) from the destination ACL, leaving the ACL empty. (The effect is the same as removing the ACL itself.)
- Detach the affected policy-map(s) from all the attached VLAN(s) and SVIs, remove the ACL from the policy-map(s), and then *reattach* the policy-map(s) back to the original SVIs.

- CSCsj27896

When a class-map entry is added or modified, a delay of several seconds can occur if the switch already has many policy maps defined. For example, a 6-second delay occurs when a new class map is added to the a switch that already has 400 hierarchical QoS policies defined.

The delay occurs even if the policy maps are not attached to a switch interface. The console might also be unresponsive when this occurs.

There is no workaround.

- CSCsj41522
The MAC addresses of routed interfaces on a platform might change following a reload.
There is no workaround.
- CSCsj52956
In Cisco IOS Release 12.2(37)SE or later, the TxBufferFullDropCount counter always increments even when the switch is a standalone switch.
There is no workaround.
- CSCsj53001
In Cisco IOS Release 12.2(37)SE or later, the *Total output drops* field in the **show interfaces** privileged EXEC command output displays ASIC drops.
 - On some interfaces, the *Total output drops* field is always 0 even though the **show platform port-asic stats drop** privileged EXEC command output shows ASIC drops.
 - The *Total output drops* value is the same for all the ports that are linked to the same ASIC.
 There is no workaround.
- CSCsj64054
When REP is configured on an EtherChannel that has the channel protocol mode as ON and the primary physical link is removed from the Etherchannel interface, the REP link goes down.
The workaround is to also remove the physical link on the peer Etherchannel interface, and then enter the **shutdown** and then **no shutdown** interface configuration commands on the port channel interface.
- CSCsj83197
When REP is configured on a VLAN and you disable MAC address per-VLAN learning on that VLAN by entering the **no mac address-table learning vlan *vlan-id*** global configuration command, it can cause MAC addresses on the VLAN to flap and the Layer 3 protocol to go down.
The workaround is not to not use the **no mac address-table learning vlan *vlan-id*** command. If the command has been used then disable the command by entering the **default mac address-table learning vlan *vlan-id*** global configuration command. When MAC address per-VLAN learning and REP are configured on the same VLAN, it can cause MAC addresses on the VLAN to flap and the Layer 3 protocol to go down.
- CSCsj86231
When you try to apply a service policy to an interface, you might see this error message:

```
QoS: Error setting QinQ policy, error in allocating NP memory
QoS: Failed to upload service policy for port Gi1/1/2 Service Policy attachment failed.
```

 This can occur when the allowed number of match records is exceeded.
The workaround, if you see this error, is to not use a match statement in an IEEE 802.1Q tunneling class-map in the policy-map that would result in more than 4096 tunneling match records for the tunneling pair.
- CSCsj99343
When you make a topology change in the REP ring segment, the MPLS flows on the switch might take several seconds to recover.
There is no workaround.

- CSCsk00716
The Resilient Ethernet Protocol (REP) convergence times on a ring might be longer when a cable is pulled from an enhanced services port that has a large number of VLANs.
There is no workaround.

Resolved Caveats

These sections describe the caveats that have been resolved in this release:

- CSCsg36159
The qualified **queue-limit** policy-map class configuration command is now processed correctly for QOS-group values between 17 and 99, and the hardware is programmed to set up the queue limit threshold for the QOS-groups.
- CSCsg63499
The **trust ip-precedence class** configuration command is now correctly rejected by the switch because it is not supported in a hierarchical service policy on an enhanced-services port.
- CSCsi64513
When Ethernet Local Management Interface (E-LMI) is enabled on an enhanced-services port and VLAN translation is also configured for some VLANs on the port, VLAN translation processes and the VLANs are no longer error-disabled by E-LMI.
- CSCsh30966
This message no longer appears when the ternary content addressable memory (TCAM) is full:
%PLATFORM_PM-3-HOSTACCESSFAIL: Unable to configure hardware to restrict host access on Fa1/0/47. Port may not behave as expected.
- CSCsh96763
A Catalyst 3750 Metro switch no longer sends packets out the wrong interface or with an incorrect label in a Multiprotocol Label Switching (MPLS) VPN environment.
- CSCsi08513
MAC flap-notification no longer occurs when a switch is running VLAN bridge spanning-tree protocol (STP) and fallback bridging is configured on the VLANs running STP.
- CSCsi10584
Multiple Spanning-Tree Protocol (MSTP) convergence time has been improved for Cisco IOS Release 12.2.
- CSCsi75246
An address learned as a supplicant that is aged out by port security aging is now correctly relearned by port security under any of these conditions:
 - IEEE 802.1x authentication, port security, and port security aging are enabled on a port.
 - An address is cleared by port security.
 - You enter the **clear port security** privileged EXEC command.

- CSCsj79324

In Cisco IOS Release 12.2(37)SE, when the **set mpls experimental x** policy-map class configuration command is in a policy map, attaching the policy map to an interface no longer fails, and a message such as this no longer appears:

```
QoS: Invalid action 'trust' in class xxxx, policy xxxxx QoS: Invalid action in class
xxxx, policy xxxxx
```

Documentation Updates

This section contains these documentation updates:

- [Update to Software Configuration Guide and Command Reference, page 23](#)
- [Update to Software Configuration Guide, page 23](#)
- [Updates to System Message Guide, page 25](#)
- [Changed System Messages, page 26](#)
- [Updates to the Hardware Installation Guide, page 26](#)

Update to Software Configuration Guide and Command Reference

In the “Configuring Resilient Ethernet Protocol” chapter in the software configuration guide, and in the command reference, the allowed range for the **rep admin vlan *vlan-id*** global configuration command is shown as 1 to 4094. The correct range is 2 to 4094. To set the admin VLAN to 1, enter the **no rep admin vlan** global configuration command to return it to the default.

Update to Software Configuration Guide

QoS

As stated in the software configuration guide in Chapter 32, “Configuring QoS,” the maximum shaping limit is not limited to 1 Gigabit if an absolute parameter policy is used, but instead it depends on the link status. The implicit shaper is now 1 Gigabit if one ES link is up and 2 Gigabits if both links are up.

Note that if there are child policies under a parent shaper that contain absolute bandwidth configurations and these policies become invalid because of ES link status changes, the entire policy is removed. Absolute values are not changed internally as percentage values are. If you want to configure an EtherChannel policy for a redundant application so that all policies would hold true no matter what the link state, there are two options:

- Configure a policy without a shaper (since the switch supports only absolute shapers) and enter all bandwidth and policing in percentages. This way, the percentages will stay the same and the actual values will be automatically adjusted based on ES link status.
- Configure an absolute parameter policy that allows a combination of shaping, bandwidth and policing at various layers, making sure that all policies are derived with an implicit 1 Gigabit shaper. One easy way to do this is to force one ES link down and make sure that the other one is UP. Then configure and attach a policy. If that policy is accepted and attached, this will remain the same if either link is down or if both links are up. The best effort traffic, or traffic that does not match the policy will occupy the remaining bandwidth.

Supported MIBs

Cisco IOS Release 12.2(40)SE adds support for this MIB:
CISCO-IPSLA-ETHERNET-MIB

Unsupported Embedded Event Manager Commands

Privileged EXEC

event manager scheduler clear
event manager update user policy
show event manager detector
show event manager version

Global Configuration

event manager detector rpc
event manager directory user repository

Applet Configuration (config-applet)

event rpc
event snmp-notification
trigger (EEM)

Trigger Applet Configuration (config-applet-trigger)

attribute (EEM)
correlate

Event Trigger Configuration (config-event-trigger)

event owner

Updates to System Message Guide

These system messages were added to this release:

Error Message DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. [enet] is the supplicant MAC address, and [chars] is the interface. This message might appear if the IEEE 802.1x feature is enabled.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, manually remove it from that port.

Error Message SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].

Explanation The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

Error Message ESF_API-3-MTU_SET_FAILED

Explanation An internal error prevents the switch from configuring the jumbo maximum transmission unit (MTU) setting on the enhanced-services ports.

Recommended Action No action is required.

Error Message PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message REP-4-LINKSTATUS: [chars] (segment [dec]) is [chars]

Explanation The Resilient Ethernet Protocol (REP) link status has changed. The first [chars] is the interface name that has a link-status change. The [dec] is the REP segment number of the interface. The second [chars] is the new link status.

Recommended Action No action is required.

Error Message REP-5-PREEMPTIONFAIL: can not perform preemption on segment [dec] due to [char]

Explanation The Resilient Ethernet Protocol (REP) preempt operation failed. This could be due to an invalid port ID or a neighbor_offset number specified with the **rep block port** interface configuration command. This could also be caused by entering the **rep block port preferred** interface configuration command if there is no REP port configured with the **preferred** keyword. [dec] is the segment number, and [char] is the reason for the failure.

Recommended Action Correct the configuration, and run REP manual pre-emption on the primary edge port by entering the **rep preempt segment** command.

Changed System Messages

This system message has changed (both explanation and action).

Error Message EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration.

Updates to the Hardware Installation Guide

These sections list updates to the hardware installation guide:

- [Installation Update, page 27](#)
- [Chapter 3 “Connecting the Power Supply”, page 27](#)
- [Appendix A “Technical Specifications”, page 27](#)

Installation Update

Cisco Ethernet Switches are equipped with cooling mechanisms, such as fans and blowers. However, these fans and blowers can draw dust and other particles, causing contaminant buildup inside the chassis, which can result in a system malfunction.

You must install this equipment in an environment as free as possible from dust and foreign conductive material (such as metal flakes from construction activities).

These standard provide guidelines for acceptable working environments and acceptable levels of suspended particulate matter:

- Network Equipment Building Systems (NEBS) GR-63-CORE
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20

Chapter 3 “Connecting the Power Supply”

Preparing for Installation

Locate the terminal block plug that ships with the DC power supply.

Obtain these necessary tools and equipment:

- Ratcheting torque screwdriver with a Phillips head that exerts up to 15 pound-force inches (lbf-in.) of pressure
- Panduit crimping tool with optional controlled cycle mechanism (model CT-700, CT-720, CT-920, CT-920CH, CT-930, or CT-940CH)
- 6-gauge copper ground wire (insulated or noninsulated)
- Four leads of 18-gauge copper wire. The DC terminal block also accepts 12-28 AWG copper wire.



Note We recommend that you use 18 AWG copper wiring for Network Equipment Building Systems (NEBS) installations. This guideline follows the standard guidelines for DC power wiring in the Central Office.

- Wire-stripping tools for stripping 6- and 18-gauge wires

Appendix A “Technical Specifications”

These are the correct weights for the Catalyst 3750 Metro switches:

- Catalyst 3750 Metro 24-AC switch with one AC power supply: 12.1 lb (5.5 kg)
- Catalyst 3750 Metro 24-AC switch with two AC power supplies: 14.0 lb (6.35 kg)
- Catalyst 3750 Metro 24-DC switch with one DC power supply: 12.0 lb (5.44 kg)
- Catalyst 3750 Metro 24-DC switch with two DC power supplies: 13.8 lb (6.26 kg)

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 listed in the “[Obtaining Documentation, Obtaining Support, and Security Guidelines](#)” section on page 29.

- *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=)
- These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

© 2007-2009 Cisco Systems, Inc. All rights reserved.

