Release Notes for the Catalyst 3750 Metro Switch Cisco IOS Release 12.2(50)SE and Later

Revised October 5, 2010

Cisco IOS Release 12.2(50)SE and later runs on the Catalyst 3750 Metro switch.

These release notes include important information about Cisco IOS Release 12.2(50)SE 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 38.

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:

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

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
	DOM[5] support for GLC-BX, CWDM, and DWDM SFPs	Cisco IOS Release 12.2(44)SE
	1000BASE-LX/LH MMF and SMF 1000BASE-SX MMF DOM support for GLC-ZX-SM SFP, 1000BASE-LX/LH, and 1000BASE-SX	Cisco IOS Release 12.2(46)SE
	Additional DWDM SFP qualifications	Cisco IOS Release 12.2(50)SE

For a complete list of supported SFPs and part numbers, see the Catalyst 3750 Metro data sheet at:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5532/product_data_sheet0900aecd806e27b9.html

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

Upgrading the Switch Software

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.122-50.SE5.tar	Cisco IOS image tar file. This image has Layer 2+ and Layer 3 features.
c3750me-i5k91-tar.122-50.SE5.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.122-50.SE.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

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:

- Bidirectional Forwarding Detection (BFD) Protocol to quickly detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols.
- REP configuration on edge ports connected to ports that do not support REP.
- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- CPU utilization threshold trap monitors CPU utilization.
- Support for Embedded Event Manager Version 2.4.
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Support for the CISCO-ENTITY-SENSOR MIB and the CISCO-PORT-QOS-MIB

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
BFD	12.2(50)SE
REP support on ports connected to nonREP ports	12.2(50)SE
NEAT with 802.1X switch supplicant, host authorization with CISP, and auto enablement	12.2(50)SE
CPU utilization threshold trap	12.2(50)SE

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

Feature	Minimum Cisco IOS Release Required
EEM 2.4	12.2(50)SE
RADIUS server load balancing	12.2(50)SE
REP timer and counter enhancements	12.2(46)SE
MPLS traffic engineering and fast reroute	12.2(46)SE
HSRPv2	12.2(46)SE
EOT and IP SLAs EOT static route	12.2(46)SE
DHCP server port-based address allocation	12.2(46)SE
DHCP-based autoconfiguration and image update	12.2(44)SE
Configurable small-frame arrival threshold	12.2(44)SE
Source Specific Multicast (SSM) mapping for multicast applications	12.2(44)SE
Support for the *, *ip-address*, **interface** *interface-id,* and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command	12.2(44)SE
Flex Link Multicast Fast Convergence	12.2(44)SE
IEEE 802.1x readiness check	12.2(44)SE
Configurable control-plane queue assignment	12.2(44)SE
Prioritization of management traffic	12.2(44)SE
/31 bit mask support for multicast traffic	12.2(44)SE
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

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

Feature	Minimum Cisco IOS Release Required
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
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

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

Feature	Minimum Cisco IOS Release Required
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

- 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)

- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

EtherChannel

- 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.(CSCsh12472)

Fallback Bridging

- 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)

Hot Standby Routing Protocol (HSRP)

- 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

- 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

- 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)

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).

MAC Addressing

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)

Multiprotocol Label Switching (MPLS) and Ethernet over MPLS (EoMPLS)

- 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)
- CSCsl65914

  When you mark SNMP packets to an IP DSCP value setting, and you then mark the control plane protocol packets to a different CPU traffic quality of service (QoS) value setting, the CPU traffic setting overrides the SNMP IP DSCP setting.

This only occurs on the enhanced services ports with Multiprotocol Label Switching (MPLS) configured. The Fast Ethernet and Gigabit Ethernet customer edge ports are not affected.

There is no workaround. You can specify the marking as either SNMP IP DSCP or as CPU traffic QoS, not both.

- For pseudowire redundancy, the switch does not support LDP MAC address withdrawal.

  There is no workaround. (CSCsq24540)

Multicasting

- 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)
- A switch drops unicast traffic under these conditions:
  - The switch belongs to a Layer 2 ring.
  - More than 800 Mbps of multicast traffic is sent in both directions on the interface.

  When multicast traffic is sent in one direction and unicast traffic is sent in another, unicast traffic is dropped at the multicast traffic source port.

  The workaround is to apply a policy map so that the least significant traffic is discarded. (CSCsq83882)

Quality of Service (QoS)

- 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)

- You cannot enable MPLS fast reroute (FRR) link protection notifications by using SNMP (via the cmplsFrrNotifsEnabled object in the CISCO-MPLS-FRR-MIB).

  The workaround is to use the CLI to enable the trap by entering the **snmp-server enable traps mpls fast-reroute** [**protected**] global configuration command. (CSCsq07065)

Resilient Ethernet Protocol (REP)

- 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. (CSCsk00716)

- Although you can configure a REP segment without configuring REP edge ports, we recommend that you configure REP edge ports whenever possible because edge ports enable these functions:
  - selecting the preferred alternate port
  - configuring VLAN load balancing
  - configuring topology change notifications (TCNs) toward STP, other REP segments, or an interface
  - initiating the topology collection process
  - preemption mechanisms

  You cannot enable these functions on REP segments without edge ports.

Routing

- 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)

- The MAC addresses of routed interfaces on a platform might change following a reload.

  There is no workaround. (CSCsj41522)

SPAN and Remote SPAN (RSPAN)

- 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)

- 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 problems occurs if the egress port is a switch port on a Catalyst 3750 switch.

  There is no workaround. (CSCsj21718)

Trunking

- 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

- 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

- 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

- Cisco IOS Release 12.2(50)SE introduces the virtual circuit (VC) auto-sense signaling feature for hierarchical virtual private LAN service (H-VPLS), the xconnect of the SVI, to interoperate with the ASR 9000 Series routers. The default signaling for H-VPLS is now VC type 5. The local Catalyst 3750 Metro PE switch boots up signaling for VC type 5. If the remote PE switch also supports type 5, H-VPLS comes up with type 5. If the remote switch supports only VC type 4, the local PE switch resets and renegotiates for VC type 4, and the H-VPLS comes up with type 4. Therefore, H-VPLS comes up whether the remote PE supports VC type 4 or VC type 5. The behavior before Cisco IOS Release 12.2(50)SE was that H-VPLS would not come up unless remote PE also supported VC type 4.

  By definition, the local PE H-VPLS VLAN should not be relevant for the VPLS network. Because the local PE SVI with the xconnect and the remote PE SVI with the xconnect do not need to be on the same VLAN, it does not matter if the VLAN is carried across the transport network or not. However, problems could occur if a service provider deployed the Catalyst 3750M switch using the H-VPLS VLAN as the customer VLAN when H-VPLS came up with VC type 5 because the customer VLAN tag would not be consistent across the transport. The new behavior is now consistent with the Cisco default.

- 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 an 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

- 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.

- CSCsw68528

  On switches running Cisco IOS Release 12.2(44)SE or 12.2(46)SE, when you enter the **show mvr interface** *interface-id* **members** privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as *ACTIVE*.

  The workaround is to use the **show mvr interface** *interface-id* or the **show mvr members** privileged EXEC command. These command outputs show the correct status of an MVR port.

- CSCsw69015

  When you enter the **mvr vlan** *vlan-id* global configuration command to create an MVR VLAN and enable MVR on the switch by entering the **mvr** global configuration command, if you enter the **show mvr interface** *interface-id* **members** privileged EXEC command, the output shows the MVR groups on the interface. However, if you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly.

  The workaround, if the groups are not displaying correctly, is to create the MVR VLAN *before* enabling MVR. The configuration then displays correctly.

- CSCta39090

  On an enhanced services (ES) port where you have configured bandwidth by entering the **bandwidth** *value* policy configuration command for a hierarchical policy, When a traffic stream bandwidth reservation is for a low rate (that is, less than 100 kb/s), the reservation is honored. However, the stream can become very bursty under congestion, especially when other streams at the same level of the QoS hierarchy are reserving substantially more bandwidth.

  There is no workaround.

- CSCta57846

  The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

  The workaround is to enter the **logging file flash**:*filename* global configuration command to configure logging to flash instead of copying to flash.

- CSCti79385

  When a redirect URL is configured for a client on the authentication server and a large number of clients are authenticated, high CPU usage could occur on the switch.

  There is no workaround.

Resolved Caveats

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE5

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE4

- CSCsh59019

  Authentication, authorization, and accounting (AAA) fails, preventing authentication and requiring you to recover your password. For example, when you enter the **aaa authentication login default group tacacs line** global configuration command, AAA fails.

  There is no workaround.

- CSCsk85192

  When you use an access control server (ACS) to enable command authorization, the ACS does not process a **copy** command ending with a colon (for example, *scp***:**, *ftp***:**, *tftp***:**, *flash***:**).

  This problem affects authentication, authorization, and accounting (AAA) authorization:

  - If the ACS denies a **copy** command ending with a colon, you *can* use that command on a switch.
  - If the ACS permits a **copy** command ending with a colon, you *cannot* use that command on a switch.

  To workaround is to either deny or permit the **copy** command without entering any arguments on the ACS.

- CSCsx31345

  After you enter the **snmp mib rep trap-rate** global configuration command on a switch that is configured for Resilient Ethernet Protocol (REP) and link-state tracking (LST) and you shut down or disconnect all LST upstream links, a memory allocation failure occurs.

  There is no workaround.

- CSCsx97605

  The CISCO-RTTMON-MIB is not correctly implemented in this release.

  There is no workaround.

- CSCsy83366

  On a switch that is configured for quality of service (QoS), a memory leak occurs when a small portion (about 90 bytes) of the processor memory is not released by the HRPC QoS request handler process.

  There is no workaround.

- CSCta09189

  Packet loss and output drops occur on the egress interface for routed multicast traffic.

  This problem occurs when multiple S,G entries time out at the same time and then are re-established at the same time, when multiple Protocol Independent Multicast (PIM) neighbors time out at the same time and then are re-established at the same time, or when multiple high-volume multicast streams are routed through multiple Layer-3 interfaces.

Use one of these workarounds:

- Enter the **clear ip mroute *** EXEC command.
- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the egress interface.

- CSCtb10158

  A switch can fail when an SNMP process attempts to configure dot1x authentication when it is already configured.

  There is no workaround.

- CSCtb77378

  When you use IEEE 802.1x authentication with web authentication and an HTTP page opens, the switch redirects the user to an HTTP login page, not a HTTPS login page.

  The workaround is to remove the custom banner.

- CSCtb78951

  Memory allocation failures occur on a Metro Ethernet switch that is configured for Resilient Ethernet Protocol (REP) and that has poor point-to-point physical link integrity with a neighboring REP node. These failures are caused by I/O memory fragmentation and can result in REP-4-LINKSTATUS error messages, REP control Protocol Data Unit (PDU) packet loss, or both.

  The workaround is to ensure that the physical link with the neighboring REP node is good.

- CSCtb91572

  A switch enters a loop in which it continues to fail after it first has failed while starting, and then has failed again while attempting to recover. This failure loop occurs only after you have entered the **archive upload-sw** privileged EXEC command to write the configuration to a remote server using Secure Copy Protocol (SCP) and when the connection to the remote server is configured for spanning-tree PortFast.

  The workaround is to not use SCP to write to the remote server. Use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

- CSCtc39809

  A memory leak occurs when there is a stuck in active (SIA) state condition for an Enhanced Interior Gateway Routing Protocol (EIGRP) route.

  There is no workaround.

- CSCtc43231

  A switch does not receive SNMP trap and inform messages from the correct interface after you have entered the **snmp-server trap-source loopback0** and **snmp-server source-interface informs loopback0** global configuration commands.

  There is no workaround.

- CSCtc53456

  This error message frequently appears on a Catalyst 3750 Metro switch that has a single power supply:

  ```
  %POWER_SUPPLIES-5-PWR_OK: Power supply B is functioning
  ```

  There is no workaround.

- CSCtc57809

  When the **no mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command is used to remove a dynamically learned MAC address, the switch fails under these conditions:

  – The physical interface is in a *no shut* state.

  – The MAC address is first dynamically learned and then changed to static.

  There is no workaround.

- CSCtc70571

  When you have configured an output service policy, performing an SNMPWALK on cportQosStatistics causes loops.

  There is no workaround.

- CSCtc90039

  A memory leak occurs on a device that uses Enhanced Interior Gateway Routing Protocol (EIGRP) when the external routes are being exchanged.

  The workaround is to stabilize the network to minimize the impact of external route advertisement.

- CSCtd17296

  When you enter the **dot1x pae** interface configuration command on a switch access port and then enable an access list in the inbound direction on an ingress switched virtual interface (SVI), the access list does not work, allowing all packets to pass.

  The workaround is to enable the access list in the outbound direction on the egress SVI.

- CSCtd30053

  When you enter the **no spanning-tree etherchannel guard misconfig** global configuration command, enter the **write memory** privileged EXEC command, and then restart the switch, the **spanning-tree etherchannel guard misconfig** global configuration command is saved instead of the **no** form of this command.

  There is no workaround.

- CSCtd31242

  An IP phone loses network connectivity under these conditions:

  – The IP phone is authenticated by MAB (in Open1x mode) on a supplicant switch.

  – The supplicant switch is connected to an authenticator switch through the NEAT protocol.

  A call is placed using the IP phone. After approximately 5 minutes, network connectivity to the phone is lost.

  The workaround is to statically configure the MAC address of the IP phone on the authenticator switch.

- CSCtd34310

  After receiving an invalid Edge/End Port Advertisement (EPA), a switch that is configured for Resilient Ethernet Protocol (REP) fails because of a watchdog time-out.

  Before the switch fails, it generates messages such as this:

  ```
  SYS-3-CPUHOG: Task is running for (528552)msecs, more than (2000)msecs (66/0),process
  = REP BPA/EPA Proc.
    -Traceback=
  ```

  There is no workaround.

- CSCtd50287

  After Resilient Ethernet Protocol (REP) has converged among several switches, multicast traffic is no longer flooded to one switch.

  The workaround is to enter the **set igmp querier** privileged EXEC command.

- CSCtd72456

  After you have entered the **snmp-server host informs** global configuration command to enable SNMP informs on a switch, the switch might fail if you enter the **show snmp pending** user EXEC command.

  There is no workaround. Do not enter the show command when SNMP informs are enabled.

- CSCtd72626

  A Remote Switched Port Analyzer (RSPAN) does not detect IPv6 multicast packets on an RSPAN destination port.

  There is no workaround.

- CSCtd73256

  A switch fails when you enter the **show ip ospf interface** user EXEC command and then stop the command output at the this line:

  ```
  Backup Designated router (ID) xx.x.x.x, Interface address xx.x.x.x
  ```

  The failure occurs when the Backup Designated Router (BDR) neighbor of the switch is shut down while you press Enter or the spacebar to advance the command output.

  When the switch fails, it sends this error message:

  ```
  Unexpected exception to CPUvector 2000, PC = 261FC60
  ```

  There is no workaround.

- CSCte67201

  On a switch that is configured for IP routing and that is running Cisco IOS Release 12.2(50)SE or later, Cisco Express Forwarding (CEF) can use a large amount of memory. The IP RIB Update process uses about 2000 bytes for each prefix that CEF uses.

  There is no workaround. You can reduce the memory use by reducing the number of routes the switch processes.

- CSCte81321

  After you have entered the **logging filter** global configuration command on a switch to specify a syslog filter module to be used by the Embedded Syslog Manager (ESM), processes logging many system messages retain increasing amounts of processor memory.

  The workaround is to enter the **no logging filter** global configuration command.

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE3

- CSCsl72774

  Memory allocation errors no longer occur when the Cisco Express Forwarding (CEF) consistency checkers have been enabled. The CEF consistency checkers have been enabled by default. They can also be enabled by using these global configuration commands:

  cef table consistency-check ipv4

  cef table consistency-check ipv6

- CSCso57496

  A switch no longer fails when you enter the **configure replace** privileged EXEC command, and a banner is already present in the switch configuration.

- CSCso90107

  You can now query the bgpPeerTable MIB for VPN/VRF interfaces.

- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

- CSCsq51052

  The output of the **show ip ssh** privileged EXEC command no longer displays *SSH Enabled - version 2.99*. Instead, a correct SSH version (*1.5*, *1.99* or *2.0*) now appears.

- CSCsw45277

  Third-party IP phones now automatically power up when reconnected to enabled PoE ports on the switch.

- CSCsx49718

  Re-authentication now occurs on a port under these conditions:

  – The port is in single-host mode.

  – The port is configured with the **authentication event no-response action authorize vlan** *vlan-number* command.

  – An EAPOL start packet is sent to the port.

- CSCsx70889

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCsy07555

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCsy15227

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

- CSCsy48370

  The switch no longer fails when you use the **vacant-message** line configuration command.

- CSCsy62606

  The switch no longer has high CPU usage due to adjacency entries that were not programmed in hardware.

- CSCsy66686

  The switch no longer reloads when the default port cost of service (CoS) value is updated on a port that has a policy map configured and CoS override enabled with the **mls qos cos override** privileged EXEC command.

- CSCsy72669

  If a link failure occurs on a secondary edge port, preemption now occurs after the link comes up.

- CSCsy91579

  A switch no longer randomly resets due to memory corruption.

- CSCsz12381

  When open1x authentication and MAC authentication bypass are enabled on a port, an IP phone is connected to the port, and DHCP snooping is enabled on the switch, DHCP traffic is now forwarded on the voice VLAN before open 1x authentication times out and the switch uses MAC authentication bypass to authorize the port.

- CSCsz13490

  The switch no longer reloads when you enter several key strokes while in interface-range configuration mode.

- CSCsz14369

  If MAC authentication bypass is enabled and the RADIUS server is not available, the switch now tries to re-authenticate a port after a server becomes available.

- CSCsz19002

  IPv6 multicast packets are no longer forwarded between two isolated ports in the same private VLAN.

- CSCsz79652

  A memory leak no longer occurs when Cisco Network Assistant is polling the switch and the **ip http server** or **ip http-secure-server** global configuration command is enabled.

- CSCsz81762

  If you enable automatic server testing through the **radius-server host** *ip-address* [**test username** *name*] global configuration command, the switch no longer sends requests to the RADIUS server if the server is not available.

- CSCta36155

  A switch configured with 802.1x and port security on the same ports no longer might inappropriately put the ports into an error-disabled state.

- CSCta56469

  Moving a PC between two IP Phones without disconnecting either phone from the switch no longer triggers a port-security violation.

- CSCta67777

  A port security violation error no longer occurs when MAC address sticky learning is enabled on a port and a CDP is enabled on a connected IP Phone.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE1

- CSCsb46724

  If the connection to a primary AAA server fails, the backup server is now queried for login access.

- CSCsr92741

  When a TCP packet with all flags set to zero (at the TCP level) is sent to a remote router, the remote (destination) router no longer returns an ACK/RST packet back to the source of the TCP segment.

- CSCsy24510

  The switch now accepts an encrypted secret password.

- CSCsy46727

  The switch now correctly forwards IPv4 multicast control packets.

- CSCsy76409

  Packets are no longer corrupted when sent through a pseudowire interface.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE

- CSCsi70454

  The configuration file used for the configuration replacement feature requires the character string *end\n* at the end of the file. The Windows Notepad text editor does not add the *end\n* 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 *end\n* 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 now correctly to re-attaches to the SVI.

- CSCsj99343

  When you make a topology change in the REP ring segment, the MPLS flows on the switch no longer take several seconds to recover.

- CSCsq26873

  The server no longer attempts re-authentication every ten minutes when a switch is configured with the **dot1x timeout reauth-period server** interface configuration command.

- CSCsq67398

  Traffic is now forwarded to the interfaces that are configured with static multicast MAC addresses after the switch is reloaded.

Note You cannot configure the static MAC address (unicast or multicast) entries on EtherChannel member interfaces, or add an interface into the EtherChannel if that interface is associated with a static MAC address entry.

- CSCsq89564

  If the switch uses 802.1x authentication with VLAN assignment, it no longer uses the VLAN assignment with different authorization attempts, such as user authentication or re-authentication.

- CSCsr40488

  When a Catalyst 3750 Metro switch is a Layer 2 Virtual Private Network (VPN) provider-edge (PE) device and has a port-channel interface at customer-edge (CE) site, this message no longer appears if the physical port-channel interface is down:

```
*Mar 3 22:55:56.040: %LINK-3-UPDOWN: Interface FastEthernet1/0/13, changed state to up
*Mar 3 22:55:57.046: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/13, changed state to up
*Mar 3 22:55:57.046: L2VPN: Can't set special DI on port channel member port Fa1/0/13
```

- CSCsr50766

  When keepalive is disabled on an interface, the interface is no longer put in an error-disabled state when it receives keepalive packets.

- CSCsr64007

  The Switched Port Analyzer (SPAN) destination port no longer detects IPv6 multicast packets from a VLAN that is not being monitored by SPAN.

- CSCsr65689

  This message no longer appears in the log during the system bootup on a switch that is running Cisco IOS 12.2(50)SE:

```
%COMMON_FIB-3-FIBIDBINCONS2
```

- CSCsu10065

  When SFP ports are configured as status multicast router ports, IPv6 Multicast Listener Discovery (MLD) snooping now works after the switch reloads.

- CSCsu51381

  When you reload the switch by using the **reload** privileged EXEC command, the enhanced-services (ES) ports are put in the down state to prevent a connected device running UDLD on the link from reporting a UDLD failure while the switch reloads.

- CSCsu59214

  The *Set TxPortFifo SRR Failed* message no longer appears when you enter both the s**rr-queue bandwidth shape 200 0 2 200** and the **priority-queue out** interface configuration commands on the same interface.

- CSCsu64565

  The switch no longer fails when you define an unsupported traffic class in a non-hierarchical QoS policy map that is attached to an ingress ES port.

- CSCsu68538

  When the Multiprotocol Label Switching (MPLS) forwarding table has more than 7000 entries, entries with the /32 prefix are now programmed into hardware.

- CSCsu88168

  The switch no longer reloads when the Forwarding Information Base (FIB) adjacency table is added.

- CSCsv04568

  On the Catalyst 3750 Metro switch, model 3750-24TE, abnormally high CPU usage no longer occurs during periods of high levels of background processing.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website 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-20090908-tcp24.shtml.

- CSCsv30429

  A Cisco IP Phone connected to a Catalyst switch no longer becomes unauthorized when it transitions from the data authorization domain to the voice authorization domain.

- CSCsv64023

  A switch port configured for IGMP snooping no longer lose its group membership when the port receives a query comes from an upstream device that is not configured for IGMP snooping.

- CSCsv65793

  The switch no longer fails after you configure a multicast VLAN registration (MVR) group.

- CSCsv89005

  A switch configured with class-based policies that are applied and active on at least one interface no longer might reload or display CPU hog messages during SNMP polling for the ciscoCBQosMIB.

- CSCsv91358

  When you have entered the **vlan dot1q tag native** global configuration command to configure a switch to tag native VLAN frames on 802.1Q trunk ports, and you configure a new voice VLAN on an access port, the MAC address of a connected PC is now correctly relearned.

- CSCsw30249

  When a switch virtual interface (SVI) is configured as unnumbered and is pointing to a loopback interface, the switch no longer fails when the SVI receives a packet.

- CSCsw45337

  When LLDP is enabled and a voice VLAN is configured, the L2 Priority and DSCP Value fields in the LLDP type, length, and value descriptions (TLVs) are now correctly marked to give the voice traffic the correct DSCP and Layer 2 priority.

- CSCsw65548

  Switch ports no longer attempt authentication at the interval configured for the port security timer instead of the configured IEEE 802.1x timer.

Documentation Updates

This section contains these documentation updates:

Updates to the Software Configuration Guide

Although documented in the software configuration guide, VRF-Aware services for Unicast Reverse Path Forwarding (uRPF) is not supported.

Updates to the System Message Guide

These system messages are not yet in the system message guide:

Error Message `ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]`

Explanation There are insufficient resources available to create a hardware representation of the ACL. A lack of available logical operation units or specialized hardware resources can cause this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Recommended Action Modify the ACL configuration to use fewer resources, or rename the ACL with a name or number that alphanumerically precedes the other ACL names or numbers.

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 `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 `%PAGP_DUAL_ACTIVE-3-OBJECT_CREATE_FAILED: Unable to create [chars]`

Explanation The switch cannot create the specified managed object. [chars] is the object name.

Recommended Action No action is required.

Error Message `%PAGP_DUAL_ACTIVE-3-RECOVERY_TRIGGER: PAgP running on [chars] informing virtual switches of dual-active: new active id [enet], old id [enet]`

Explanation Port Aggregation Protocol (PAgP) received a new active ID on the specified interface, which means that all virtual switches are in a dual-active scenario. The interface is informing virtual switches of this, which causes one switch to go into recovery mode. [chars] is the interface. The first [enet] is the new active ID. The second [enet] is the ID that it replaces.

Recommended Action No action is required.

Error Message `%PAGP_DUAL_ACTIVE-3-REGISTRY_ADD_ERR: Failure in adding to [chars] registry`

Explanation The switch could not add a function to the registry. [chars] is the registry name.

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 `%PM-6-EXT_VLAN_ADDITION: Extended VLAN is not allowed to be configured in VTP CLIENT mode.`

Explanation The switch did not add a VLAN in VTP client mode.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the system message guides.

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 preemption on the primary edge port by entering the **rep preempt segment** command.

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 `%SPANTREE_VLAN_SHIM-3-ADD_REGISTRY_FAILED: Subsystem [chars] fails to add callback function [chars]`

Explanation A subsystem has added its callback functions. Use this message only for debugging. The first [chars] is the subsystem name, and the second [chars] is the function name.

Recommended Action No action is required.

Error Message `%SPANTREE_VLAN_SHIM-2-MAX_INSTANCE: Platform limit of [dec] STP instances exceeded. No instance created for [chars] (port [chars]).`

Explanation The number of VLAN spanning-tree instances has reached the allowable maximum. No more VLAN instances are created until instances are less than the maximum. [dec] is the maximum, the first [chars] is the VLAN for which an STP instance is not created, and the second [chars] is the port number.

For example, when you are configuring spanning tree and the allowable maximum is 128 instances

- If the switch has already created 128 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 200, and an STP instance for VLAN 200 is not created.
- If the switch has already created 100 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 228. The switch creates STP instances for VLAN 200 to VLAN 227, but not for VLAN 228. 200 is not created.

STP instances are also not created for the remainder of the VLANs in the range

Recommended Action Reduce the number of active spanning-tree instances by either disabling some or deleting the VLANs associated with them. To create STP instances, manually create them. If you do not, the switch automatically creates an STP instances when a VLAN is created.

For example, if the switch has already created 128 instances and you want to create an STP instance for VLAN 200, remove a spanning-tree instance with one of these commands:

- To delete one of the VLANs with an STP instance, enter the **no vlan** *vlan-id* global configuration command.
- To disable spanning tree on a per-VLAN basis. enter the **no spanning-tree** *vlan-id* global configuration command.

Then enter the **spanning-tree 200** global configuration command to create an instance for VLAN 200.

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.

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.

Deleted System Messages

These system messages have been deleted:

Error Message `ACLMGR-2-NOVMR: Cannot create VMR data structures for access list [chars].`

Error Message `DOT1X-5-INVALID_INPUT: Dot1x Interface parameter is Invalid on interface [chars].`

Error Message `DOT1X-5-SECURITY_VIOLATION: Security violation on interface [chars], New MAC address [enet] is seen.`

Error Message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [dec] to 802.1x port [chars]`

Error Message `DOT1X_SWITCH-5-ERR_VLAN_ROUTED_PORT: Attempt to assign VLAN [dec] to routed 802.1x port [chars]`

Error Message `UDLD-3-UDLD_IDB_ERROR: UDLD error handling [chars] interface [chars].`

Error Message `UDLD-3-UDLD_INTERNAL_ERROR: UDLD internal error [chars].`

Error Message `UDLD-3-UDLD_INTERNAL_IF_ERROR: UDLD internal error, interface [chars] [chars].`

Error Message UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface [chars], [chars] detected.

Error Message UDLD-6-UDLD_PORT_RESET: UDLD reset interface [chars].

Error Message UFAST_MCAST_SW-3-PROC_START_ERROR: No process available for transmitting UplinkFast packets.

Error Message UFAST_MCAST_SW-4-MEM_NOT_AVAILABLE: No memory is available for transmitting UplinkFast packets on Vlan [dec].

Error Message VQPCLIENT-2-CHUNKFAIL: Could not allocate memory for VQP.

Error Message VQPCLIENT-2-DENY: Host [enet] denied on interface [chars].

Error Message VQPCLIENT-3-IFNAME: Invalid interface ([chars]) in response.

Error Message %VQPCLIENT-2-INITFAIL: Platform-specific VQP initialization failed. Quitting

Error Message %VQPCLIENT-2-IPSOCK: Could not obtain IP socket

Error Message %VQPCLIENT-7-NEXTSERV: Trying next VMPS [IP_address]

Error Message %VQPCLIENT-7-PROBE: Probing primary server [IP_address]

Error Message %VQPCLIENT-2-PROCFAIL: Could not create process for VQP. Quitting

Error Message %VQPCLIENT-7-RECONF: Reconfirming VMPS responses

Error Message %VQPCLIENT-2-SHUTDOWN: Interface [chars] shutdown by VMPS

Error Message %VQPCLIENT-3-THROTTLE: Throttling VLAN change on [chars]

Update to the Hardware Installation Guide

This is an update to the hardware installation guide.

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

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

- *Catalyst 3750 Metro Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Metro Switch*
- *Catalyst 3750 Metro Switch Software Configuration Guide*
- *Catalyst 3750 Metro Switch Command Reference*
- *Catalyst 3750 Metro Switch System Message Guide*
- *Catalyst 3750 Metro Switch Hardware Installation Guide*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

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

  SFP 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

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.