Release Notes for the Catalyst 3750 Metro Switch Cisco IOS Release 12.2(54)SE

April 20, 2010

Cisco IOS Release 12.2(54)SE runs on the Catalyst 3750 Metro switch.

These release notes include important information about Cisco IOS Release 12.2(54)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 39.

You can download the switch software from this site:

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

Contents

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 1000 FX GLC-EX-SMG SFP	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

- Upgrading a Switch by Using the CLI, page 4
- Recovering from a Software Failure, 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-i5k91-tar.122-54.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/image-name.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by using the **/leave-old-sw** option instead of the **/overwrite** 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:

- Using the Express Setup program as described in the *Catalyst 3750 Metro Switch Getting Started Guide.*
- Using the CLI-based setup program as described in the *Catalyst 3750 Metro Switch Hardware Installation Guide*.
- Using 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, page 5
- New Software Features, page 5

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

- Support for the IEEE 802.1ad standard to provide VLAN scalability in provider networks, giving provider bridges the same functionality as Layer 2 protocol tunneling (L2PT) and QinQ bridges. See the "Configuring IEEE 802.1ad" section on page 25 and "Updates to the Command Reference for Cisco IOS Release 12.2(54)SE" section on page 33.

- CFM support on a customer VLAN (C-VLAN), which allows a customer to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on a C-VLAN component to provide a customer with visibility to network traffic on the C-VLAN. See the "Configuring CFM on C-VLAN (Inner VLAN)" section on page 30.
- Support for the IEEE CFM (IEEE 802.1ap) MIB, which can be used as a tool to trace paths, to verify and to manage connectivity, and to detect faults in a network. See the ""Supported MIBs" Appendix" section on page 32.
- There is no limit to the number of times that you can enter the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command. You can block an unlimited number, range, or sequence of VLANs. (CSCta48811)
- For the product identifier (PID) and version identifier (VID) of small form-factor pluggable (SFP) modules, the output of the **show inventory** user EXEC command displays either the correct information or Unspecified for the PID and nothing for the VID if the SFP does not have PID and VID information. (CSCsu60206)

Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release required to support 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
Support for the IEEE 802.1ad standard.	12.2(54)SE
CFM support on customer VLANs (C-VLANs).	12.2(54)SE
IEEE CFM MIB support.	12.2(54)SE
Support for Layer 2 transport over MPLS interworking for Ethernet and VLAN interworking.	12.2(52)SE
Support for IPv6 QoS trust capability.	12.2(52)SE
Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and the MAC-Address-Table.	12.2(52)SE
Support for IP source guard on static hosts.	12.2(52)SE
IEEE 802.1x User Distribution for deployments with multiple VLANs (for a group of users) to improve network scalability by load balancing users across different VLANs. The RADIUS server assigns authorized users to the least populated VLAN in the group.	12.2(52)SE
Support for Network Edge Access Topology (NEAT) for changing the port host mode and applying a standard port configuration to the authenticator switch port.	12.2(52)SE

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

Feature	Minimum Cisco IOS Release Required
Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms.	12.2(52)SE
Support for including a hostname in the option 12 field of DHCPDISCOVER packets. Identical configuration files can be sent by using DHCP.	12.2(52)SE
DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE
Connectivity fault management (CFM) Draft 8.1 compliance to bring the OAM implementation up to the new IEEE standard.	12.2(52)SE
Support for the TWAMP standard for measuring round-trip network performance between any two devices that support the protocol.	12.2(52)SE
Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping.	12.2(52)SE
Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.	12.2(52)SE
Support for IPv6 unicast routing, neighbor discovery, default router preference, DHCP server and relay, IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping. Also supports IPv6 QoS trust functionality.	12.2(52)SE
Multicast VLAN registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch is in dynamic MVR mode and a new command (**mvr ringmode flood**) to ensure that forwarding in a ring topology is limited to member ports.	12.2(52)SE
Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals.	12.2(52)SE
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
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

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

Feature	Minimum Cisco IOS Release Required
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
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

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

Feature	Minimum Cisco IOS Release Required
IEEE 802.1x accounting and MIBs (IEEE8021-PAE-MIB and CISCO-PAE-MIB)	12.2(25)EY
DHCP snooping with the option-82 information option	12.2(25)EY
DHCP snooping binding database configuration	12.2(25)EY
Dynamic ARP inspection	12.2(25)EY
EtherChannel guard	12.2(25)EY
Flex Links	12.2(25)EY
IGMPv3 snooping	12.2(25)EY
IGMP throttling	12.2(25)EY
IP source guard	12.2(25)EY
MultipleVPN Routing/Forwarding (Multi-VRF) CE	12.2(25)EY
Private VLAN	12.2(25)EY
SFP diagnostic management interface	12.2(25)EY
SSHv2 server application (cryptographic images only)	12.2(25)EY
SSL Version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)EY
Smartports macros	12.2(25)EY
Auto-QoS	12.2(25)EY
VLAN-based QoS and dual-level hierarchical policy maps on SVIs	12.2(25)EY
Matching the CoS of the inner tag for 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.

Bidirectional Forwarding Detection

- If you create a BFD session between two switches and then create an ACL that includes the **permit ip any any log-input** access-list configuration command, when you attach the ACL to one of the connecting interfaces, the BFD session goes down. If you remove the ACL from the interface, BFD comes back up.

  The workaround is to not use a **permit** ACL entry with the log option on interfaces participating in BFD. (CSCtf31731)

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)

Connectivity Fault Management (CFM)

- On a switch running CFM, continuity check messages (CCMs) received on a MEP port that are a lower level than the configured MEP level should be discarded and an error message generated, regardless of whether or not the CCM has a valid CFM multicast destination address. On the Catalyst 3750 Metro switch, CFM C-VLAN CCMs with non-CFM multicast addresses are forwarded without CFM processing and no error messages are sent.

  There is no workaround. (CSCte39713)

- When the CFM start delay timer is configured to a small value, the *Crosscheck-Up* field in the output of the **show ethernet cfm domain** privileged EXEC command and the *Mep-Up* field in the output of the **show ethernet cfm maintenance-points remote crosscheck** privileged EXEC command might appear as *No* even if the CCM is learned in the remote database.

  This is expected behavior. The workaround is to use the **ethernet cfm mep crosscheck start-delay** command to set the delay-start timer value larger than the continuity-check interval. (CSCtf30542)‘

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 Service Level Agreements (SLAs)

- When the IP SLAs configured reaction type (configured by entering the **ip sla reaction-configuration** global configuration command) is round-trip time (RTT), an RTT event causes duplicate SNMP traps.

  There is no workaround.

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 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 FastEthernet 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. (CSCsl65914)
- 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)

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.
- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1 second, the REP link flaps if the BFD interface is shut down and then brought back up.

  The workaround is to use the **rep lsl-age-out timer** interface configuration command to configure the REP LSL age timer for more than 1000 milliseconds (1 second). (CSCsz40613)

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 enhanced-services (ES) interface. The per-interface VLAN mappings remain in effect 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 will be bundled into an EtherChannel. (CSCec49520)
- Although you can enter the **switchport vlan mapping** interface configuration command on any ES port to configure VLAN mapping, VLAN mapping is only valid on trunk ports. The configuration is allowed on an access port, but does not take effect.

  The workaround is to configure the ES port as a trunk or yo use the **switchport access vlan** *vlan_id* interface configuration command to define the access VLAN for the access port. (Ctb67562)

VLAN

- If the number of VLANs times the number of trunk ports exceeds 13,000, the switch can stop.

  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 introduced 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 provider-edge 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. H-VPLS comes up whether the remote PE supports VC type 4 or VC type 5. Before Cisco IOS Release 12.2(50)SE, H-VPLS would not come up unless the remote provider edge device 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.
- CSCtf27594

  When Bidirectional Forwarding Detection (BFD) is enabled on an interface of a switch that is running Cisco IOS Release12.2(50)SE or later, Release 12.2(52)SE or later, or Release 12.2(54)SE, CPU spikes can occur once or twice per hour.

  There is no workaround.
- CSCtf77937

  When an EtherChannel is configured for 802.1ad and a channel member that is up is removed from the EtherChannel, the 802.1ad configuration is removed. However, if the port channel is shut down and then removed from the EtherChannel, the 802.1ad configuration is not removed.

The workaround is to enter the **no shutdown** interface configuration command on the port channel before removing it from the EtherChannel.

- CSCtg26822.

  When you configure a port for 802.1ad UNI by entering the **ethernet dot1ad uni s-port** interface configuration command and enter the **l2protocol peer stp lldp** command on a UNI-S port, STP and LLDP protocols are not peered between both switches.

  The workaround, when you want to peer STP and LLDP between customer and provider edge switches and to tunnel other Layer 2 protocols, is to use the **ethernet dot1ad uni c-port** interface command to configure the service provider customer-facing port as a UNI-C port and not a UNI-S port. By default on UNI-C ports, all Layer 2 protocols, including STP and LLDP are peered. For protocols to be tunneled through the 802.1ad provider network, enter the **l2protocol forward** command on the UNI-C port.

Resolved Caveats

- CSCsc42814

  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.

- CSCsl14567

  When the status of a Resilient Ethernet Protocol (REP) primary edge port changes, for example, because you enter the **no shutdown** interface configuration command, the switch sends duplicate SNMP messages for the crepPortRoleChange trap.

  There is no workaround.

- CSCsq83882

  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.

- CSCsx97605

  The CISCO-RTTMON-MIB is not correctly implemented.

- CSCsz18634

  On a switch running Cisco IOS release 12.2(46)SE, the output of the **show interfaces** privileged EXEC command shows 0 packets for port channel input and output rates.

  The workaround is to reload the switch by entering the **reload** privileged EXEC command.

- CSCtb10158

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

  There is no workaround.

- CSCtc43231

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

  There is no workaround.

- CSCtc59162

  Modifying a prefix list that is configured as an inbound or outbound distribute-list causes the EIGRP peer to resynchronize.

  There is no workaround

- CSCtd29049

  A switch with at least one configured trunk port might fail when you use the **vlan** *vlan-id* global configuration command to configure more than 950 VLANs.

  There is no workaround.

- CSCte52821

  When you enter the **no ip ftp passive** global configuration command to allow all types of FTP connections on a switch running Cisco IOS Release 12.2(52)SE, FTP sessions could disable Telnet or console connections. You can no longer use the vty.

  The workaround is to restart the switch. To prevent FTP sessions from disabling Telnet or console connections, enter the **ip ftp passive** global configuration command.

- CSCte67201

  On a switch configured for IP routing and 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 that the switch processes.

- CSCte71904

  When you use the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command on a Resilient Ethernet Protocol (REP) primary edge port to block a VLAN list on one port and then use the same command to block another VLAN list on another port, the original port number and VLAN list are not overwritten. Therefore, after you have blocked a VLAN list on one port, you cannot block another VLAN list on another port.

  There is no workaround.

- CSCtf89939

  When you have configured REP segment topology change notices (STCNs) and VLAN load balancing on an interface, entering the **shutdown** and the **no shutdown** command on the interface can cause a memory leak or can cause the switch to reload.

  There is no workaround.

Documentation Updates

The clustering chapter has been removed from the software configuration guide and the commands removed from the command reference. The Catalyst 3750 Metro switch does not support clustering.

This section contains these documentation updates:

- Updates to the Software Configuration Guide for Cisco IOS Release 12.2(54)SE, page 25
- Updates to the Software Configuration Guide for Cisco IOS Release 12.2(52)SE, page 32
- Updates to the Command Reference for Cisco IOS Release 12.2(54)SE, page 33
- Updates to the System Message Guide, page 35
- Update to the Hardware Installation Guide, page 39

Updates to the Software Configuration Guide for Cisco IOS Release 12.2(54)SE

- "Configuring IP Unicast Routing" Chapter, page 25
- "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling" Chapter—New Section, page 25 Configuring IEEE 802.1ad
- "Configuring Ethernet OAM, CFM, and E-LMI" Chapter—New Section, page 30 Configuring CFM on C-VLAN (Inner VLAN)
- "Supported MIBs" Appendix, page 32
- "Unsupported Commands" Appendix, page 32

"Configuring IP Unicast Routing" Chapter

In the section on *Configuring BFD, Disabling BFD Echo Mode:*

- The document states that you can enter the **no bfd echo** interface config command to disable echo mode and then configure the control-packet exchange rate by entering the **bfd slow-timer** global config command. This is incorrect. When BFD echo is disabled, the BFD slow-timer configuration does not apply. In a BFD session running in asynchronous mode, BFD packets are exchanged at a negotiated duration when the session is up and at the BFD slow-timer value when the session is down.
- The section also states that disabling BFD echo on an interface disables only the sending of echo packets and the receiver of an echo packet always reflects it back to the sender. This is incorrect. In the Cisco IOS implementation of BFD, when BFD echo is disabled at one end of a link, the other end of the link also does not send echo packets and does not reflect back the echo packet.

"Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling" Chapter—New Section

Configuring IEEE 802.1ad

The Catalyst 3750 Metro switch supportS QinQ, a Cisco-proprietary system to enable double-tagging to provide VLAN scalability in the provider network, and Layer 2 protocol tunneling for tunneling customer control packets. IEEE 802.1ad uses standard protocols to solve VLAN scalability in provider networks. As with QinQ, data traffic entering from the customer interface is tagged with a service-provider tag. The customer frame crosses the provider network with two tags: the inner tag is the customer tag (C-tag). and the outer tag is the service-provider tag (S-tag). Control packets appear as data inside the provider network.

See this document for a description of IEEE 802.1ad support on Cisco provider bridges with commands:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_802_1ad.html

The Catalyst 3750 Metro switch supports these IEEE 802.1ad features:

- a switchport-based model
- all-to-one bundling
- service multiplexing (complex UNI)

In IEEE 802.1ad, a switchport is configured as either a customer user-network interface (C-UNI), a service-provider UNI (S-UNI), or a network-to-network interface (NNI). Only Layer 2 interfaces can be 802.1ad ports.

- C-UNI—This port can be either an access port or an 802.1Q trunk port. The port uses the customer bridge addresses. To configure a C-UNI port, enter the **ethernet dot1ad uni c-port** interface configuration command. New keywords added to the **switchport vlan mapping** interface configuration command allow all-to-one or selective bundling capability for customer VLANs when the interface is configured as an 802.1ad trunk C-UNI port.

  On a Catalyst 3750 Metro switch, you cannot configure an ES port as a C-UNI port.
- S-UNI—This is an access port that provides the same service to all customer VLANs entering the interface, marking all C-VLANs entering the port with the same S-VLAN. In this mode, the customer's port is configured as a trunk port, and traffic entering the S-UNI is tagged. On S-UNIs, CDP and LLDP are disabled, and STP BPDU filtering and Port Fast are enabled. The port can be configured only as an access port; trunk configuration is not allowed.
  - CFM C-VLAN configuration is not allowed on an S-UNI.
  - You enter the **ethernet dot1ad uni s-port** interface configuration command to configure the port in dot1q-tunnel mode. You cannot configure an ES port as an S-UNI.
- NNI—Entering the **ethernet dot1ad nni** interface command on a trunk port creates 802.1ad EtherType (0x88a8) and uses S-bridge addresses for CPU-generated Layer 2 protocol PDUs. Only trunk ports can be NNIs. CFM C-VLAN configuration is not allowed on an NNI.

Note On a Catalyst 3750 Metro switch, you can configure 802.1ad NNIs only on ES ports. Non-ES ports can be configured as C-UNIs or S-UNIs.

See the "Updates to the Command Reference for Cisco IOS Release 12.2(54)SE" section on page 33 for a new command added for this feature.

802.1ad Configuration Guidelines

- An S-UNI must be an access port.
- An NNI must be a trunk port.
- A C-UNI can be either an access port or a trunk port.
- On the Catalyst 3750 Metro switch, configure only ES ports as NNIs. Configure only non-ES ports as UNIs.
- 802.1ad is a port-based feature. There is no global command for enabling 802.1ad. By default, without 802.1ad, all switchports are traditional 802.1Q ports.

- When 802.1ad is enabled, the tunneling of customer data frames is done in software. If the incoming BPDU rate is high, there could be some impact on CPU utilization.
- The switches do not support 802.1ad on EVCs or 802.1ad Layer 3 termination.
- The switches do not support split horizon on 802.1ad interfaces.
- You cannot enable Layer 2 protocol tunneling on 802.1ad interfaces. The features are mutually exclusive.
- Catalyst 3750 Metro switches support a mixed configuration model for 802.1ad that allows traditional Q-in-Q tunnels and 802.1ad tunnels on a bridge at the same time. When configuring a switch in mixed configuration mode, be sure to separate the broadcast domains for traditional 802.1Q tunneling and 802.1ad tunneling. To ensure functionality, do not configure 802.1ad NNI trunk ports and 802.1Q egress trunks with overlapping sets of allowed VLANs.
- By default, customer UDLD packets are tunneled on 802.1ad S-UNI ports and are processed (peered) on C-UNI ports. End-to-end UDLD is not supported on 802.1ad C-UNI ports.
- When configuring the service provider network for 802.1ad, be sure to configure 802.1ad NNIs on all interconnecting trunk ports. This is required for end-to-end functionality for customer Layer 2 PDUs in the service provider network.

Configuring 802.1ad on EtherChannels

When configuring 802.1ad on port channels, configure the EtherChannel group first, and then configure 802.1ad port configuration on the bundled port (port channel). When configured on the EtherChannel port channel, the 802.1ad configuration is applied to all ports in the port channel.

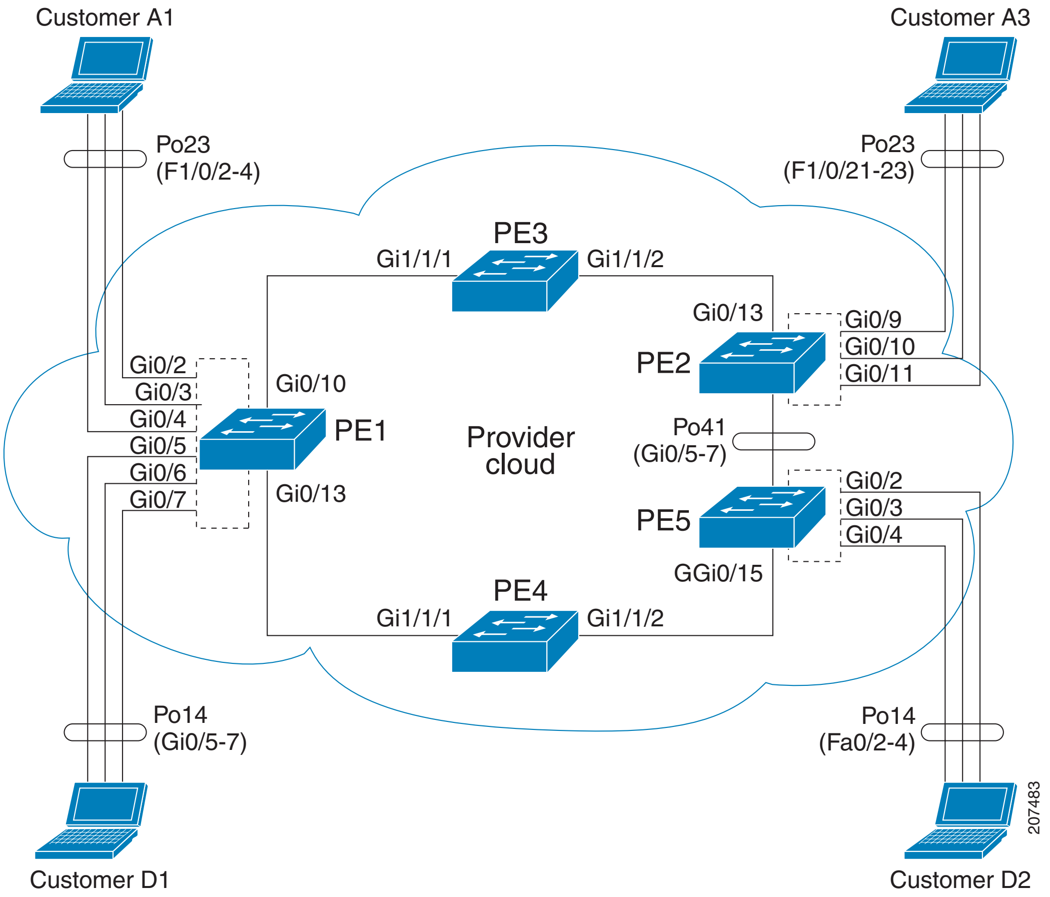
You cannot add a port to an EtherChannel if the port already has 802.1ad enabled.

Follow this configuration sequence when both CE and PE devices are actively participating in PAgP or LACP EtherChannels.

Configuration Example for 802.1ad End-to-End PAgP EtherChannels between CE Devices

For end-to-end PAgP EtherChannel tunneling between CE devices, you should extend the CE connections through the service provider network as a point-to-point service when the PE device has no EtherChannels in **on** mode. See the software configuration guide section “Configuring Layer 2 Tunneling for EtherChannels” in the “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling” chapter. The same procedure applies to 802.1ad tunnels.

Figure 1-1 802.1ad End-to-End PAgP EtherChannels



Configuration on Customer A1:

```
 Switch #show etherchannel summary
        Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        Number of channel-groups in use: 2
        Number of aggregators:           2

       Group  Port-channel  Protocol                         Ports
        ------+-------------+-----------+-----------------------------------------------
          23      Po23(SU)        PAgP (desirable)      Fa1/0/2(P)  Fa1/0/3(P)  Fa1/0/4(P)
```

Configuration on PE-1:

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# ethernet dot1ad uni s-port
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# media-type sfp
Switch (config-if)# ethernet dot1ad nni
```

Configuration on PE-3

```
Switch (config)# interface GigabitEthernet1/1/1
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk dot1q ethertype 88A8
Switch (config-if)# udld port aggressive
Switch (config-if)# ethernet dot1ad nni

Switch (config)# interface GigabitEthernet1/1/2
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk dot1q ethertype 88A8
Switch (config-if)# udld port aggressive
Switch (config-if)# ethernet dot1ad nni
```

Configuration on PE-2

```
Switch (config)# interface GigabitEthernet0/9
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/11
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/13
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# ethernet dot1ad nni
```

Configuration on Customer A3

```
Switch (config)# interface Port-channel23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk

Switch (config)# interface FastEthernet1/0/21
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable
Switch (config)# interface FastEthernet1/0/22
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config-if)# interface FastEthernet1/0/23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable
```

Configuration with 802.1ad C-UNI port on PE-2 and PE-3

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4002
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4001
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4001
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4003
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4003
Switch (config-if)# Ethernet dot1ad uni c-port
```

The configuration on other switches remains the same in the 802.1ad C-UNI scenario.

"Configuring Ethernet OAM, CFM, and E-LMI" Chapter—New Section

Configuring CFM on C-VLAN (Inner VLAN)

The previous implementation of IEEE 802.1ag CFM allows provisioning of maintenance points on the S-VLAN component. It does not allow monitoring or troubleshooting when QinQ is enabled on the provider-edge (PE) device. This release allows customers to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on the C-VLAN (inner VLAN) component of QinQ or 802.1ad ports to provide visibility on the C-VLAN. In addition, some C-VLAN restrictions are removed and C-VLANs are now supported on 802.1q tunnel ports.

For more information about this feature and the supported commands, see:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_cvlan.html

The switch supports 802.1q-tunnel-port mode

Feature Support and Behavior

CFM S-VLAN component support:

- Up MEPs at any level (0 to 7).

  Up MEPs use the port access VLAN ID (the outer tag or S-VLAN).

CFM frames sent and received by Up MEPs have a single VLAN tag, and the VLAN identifier is the port access VLAN ID (S-VLAN). Because the 802.1q tunnel interface marks the endpoint of the S-VLAN, the associated S-VLAN component should mark the endpoint of the CFM domain running over the S-VLAN space.

CFM C-VLAN component support:

- Up MEP functions at any level (0 to 7).

  Up MEPs use two tags: an outer tag with a VLAN ID that is the port access VLAN (S-VLAN) and an inner tag with a selected C-VLAN that is allowed through the 802.1q tunnel port. CFM frames sent and received by these Up MEPs are always double-tagged.

- MIP functions at any level (0 to 7).

  MIPs process CFM frames that are single-tagged when coming from the wire-side and double-tagged when coming from the relay-function side.

- Transparent point functions.

Port MEP frames are always sent untagged, even when the **dot1q vlan native** tag is enabled.

Supported maintenance points on 802.1q tunnels:

- Up MEP on the C-VLAN component for selective or all-to-one bundling
- Up MEP on the S-VLAN
- Port MEP
- MIP support on C-VLAN component for selective or all-to-one bundling

Note The switch supports only manual configuration of MIPs. It does not support MIP autocreation on C-VLANs.

Platform Restrictions and Limitations

- Maximum supported MEPs per switch at each continuity check message (CCM) interval:
  - 1600 MEP local and 1600 MEP remote (on C-VLAN and S-VLAN) with 10-second intervals
  - 250 MEP local and 250 MEP remote (on C-VLAN and S-VLAN) with 1-second intervals
  - 30 MEP local and 30 MEP remote (on C-VLAN and S-VLAN) with 100-ms intervals
- Maximum supported MIPs at each CCM interval:
  - 300 MIPs at 10 seconds
  - 125 MIPs at 1 second
  - 30 MIPs at 100 ms
- There could be issues detecting cross-connect errors on Catalyst 3750 Metro switches.
- These features are not supported:
  - CFM C-component on the native VLAN
  - Port-based and VLAN-based MPLS (pseudowire) on the C-VLAN
  - Down MEP on S or C-VLAN (provider network port)
  - MIP on S-VLAN (provider network port)
  - CFM C-VLAN alarm indication signal (AIS)

- CFM C-VLAN locked signal (LCK)
- 802.3ah interworking with CFM C-VLAN
- CFM C-VLAN IP SLAs
- CFM C-VLAN E-LMI
- CFM C-VLAN MIP autocreation.

"Supported MIBs" Appendix

The IEEE-compliant CFM MIB (IEEE CFM MIB) provides MIB support for IEEE 802.1ag compliant CFM (IEEE CFM) services. The IEEE CFM MIB can be used as a tool to trace paths, verify and manage connectivity, and detect faults in a network.

For information about the IEEE CFM MIB and the services it supports, see this URL:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_mib.html

"Unsupported Commands" Appendix

These IP unicast routing commands are now supported:

set tag (route-map configuration)

ip prefix-list (global configuration)

ip as-path access-list (global configuration)

These CGMP commands are *not* supported:

ip cgmp (interface configuration)

clear ip cgmp (privileged EXEC)

Updates to the Software Configuration Guide for Cisco IOS Release 12.2(52)SE

"Configuring IP Unicast Routing" Chapter

User Interface for VRF-Aware RADIUS

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. This release supports the **ip vrf forwarding** *vrf-name* server-group configuration and the **ip radius source-interface** global configuration commands, as described in the *Per VRF AAA Feature Guide* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

"Configuring Ethernet OAM, CFM, and E-LMI" Chapter

- This information was added:

  The Service Diagnostics 2.0 C FM diagnostic scripts is part of the 12.2(52)SE release. The script is available for download at:

  http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps9424/cisco_ios_service_diagnostics_scripts.html

Refer to the Service Diagnostic 2.0 user guide at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps9424/whitepaper_c11-566741.html

- This information was corrected:

  In the “Configuring the CFM Domain” section, Step 2 was to enter the **ethernet cfm ieee** global configuration command to configure the CFM version as IEEE 802.1ag.

  This step is not required. If you are running Cisco IOS Release 12.2(52)SE, the CFM version is always 802.1ag and the command is automatically generated when you enable CFM.

“Configuring IEEE 802.1x Port-Based Authentication” Chapter

This section was added:

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Updates to the Command Reference for Cisco IOS Release 12.2(54)SE

This platform-specific command was added for this release:

- **debug platform dot1ad**

These commands were updated:

- **rep block port, page 34**
- **show inventory, page 35**

debug platform dot1ad

To enable debugging of IEEE 802.1ad tagging, use the **debug platform dot1ad** privileged EXEC command. To disable debugging, use the **no** form of the command.

debug platform dot1ad [**error** | **events** | **receive** | **transmit**]

no debug platform dot1ad [**error** | **events** | **receive** | **transmit**]

Syntax Description

error	Displays 802.1ad error messages.
events	Displays 802.1ad event debug messages.
receive	Displays 802.1ad receive debug messages.
transmit	Displays 802.1ad sent debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(54)SE	This command was introduced.

Usage Guidelines

The **undebug platform dot1ad** command is the same as the **no debug platform dot1ad** command.

When you enter **debug platform dot1ad** with no keywords, all 802.1ad debug messages appear.

Related Commands

Command	Description
show debugging	Displays information about the enabled types of debugging.

rep block port

These usage guidelines were added:

> There is no limit to the number of times that you can enter the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command. You can block an unlimited number, range, or sequence of VLANs.
>
> When you use the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command on a Resilient Ethernet Protocol (REP) primary edge port to block a VLAN list and then use the same command to block another VLAN list on the same port, the second VLAN list does not replace the first VLAN list but is appended to the first VLAN list.

When you use the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command on a REP primary edge port to block a VLAN list on one port and then use the same command to block another VLAN list on another port, the original port number and VLAN list are overwritten.

show inventory

This usage guideline was added:

For the product identifier (PID) and version identifier (VID) of SFP modules, the output of the **show inventory** user EXEC command displays either the correct information or displays *Unspecified* for the PID and nothing for the VID if the SFP module does not have PID and VID information.

Updates to the System Message Guide

These messages were added to the system message guide:

Error Message `DOT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation The authentication was unsuccessful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action. AuditSessionID [chars]`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication. [chars] is the session ID.

Recommended Action Reduce other system activity to reduce memory demands.

Error Message `%DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Recommended Action The authentication result was overridden. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Explanation No action is required.

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was successful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars] AuditSessionID [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. This message might appear if IEEE 802.1x is enabled. [enet] is the client MAC address, the first [chars] is the interface, and the second [chars] is the session ID.

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

Error Message `DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a primary VLAN to an IEEE 802.1x port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Use a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a nonsecondary VLAN to a private VLAN host IEEE 802.1x port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the mode of the port so that it is no longer a PVLAN host port or use a valid secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the mode of the port so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN AuditSessionID [chars]`

Explanation An attempt was made to assign a data VLAN to an IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change either the voice VLAN or the IEEE 802.1x-assigned VLAN on the interface so that they are not the same.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Explanation Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Update the configuration to use a valid VLAN.

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

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the VLAN exists and is not shutdown or use another VLAN.

Deleted System Messages

These messages were deleted from the system message guide:

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action.`

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars]`

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

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

Error Message `DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars]`

Error Message `DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars]`

Error Message `DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars]`

Error Message `DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination`

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN.`

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

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

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_ON_ROUTED_PORT: Dot1x cannot assign a VLAN [dec] to a routed port [chars]`

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

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

Error Message `DOT1X_SWITCH-5-ERR_VLAN_RSPAN: Attempt to assign RSPAN VLAN [dec] to 802.1x port [chars]. 802.1x is incompatible with RSPAN`

Error Message `SW_VLAN-4-VTP_USER_NOTIFICATION: VTP protocol user notification: [chars].`

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*
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration 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.