Release Notes for the Catalyst 3750 Metro Switch Cisco IOS Release 12.2(58)SE1 and Later

Revised December 22, 2011

Note Cisco IOS Release 12.2(58)SE images for all platforms were removed from Cisco.com because of a severe defect, CSCto62631. The solution for the defect is in Cisco IOS Release 12.2(58)SE1.

Cisco IOS Release 12.2(58)SE1 runs on the Catalyst 3750 Metro switch.

These release notes include important information about Cisco IOS Release 12.2(58)SE1 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 29.

You can download the switch software from this site:

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

Contents

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

Hardware Supported

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

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

Upgrading the Switch Software

Note Before downloading software, read this section for important information.

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 2 lists the software filename for this software release.

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

Filename	Description
c3750me-i5k91-tar.122-58.SE1.tar	Cisco IOS cryptographic image tar file with 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/prod/collateral/iosswrel/ps8802/ps6969/ps1835/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*:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

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:

a. If you are a registered customer, go to this URL and log in.

   http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

b. Navigate to **Switches > Service Provider Switches - Ethernet Access**.

c. Navigate to your switch model.

d. Click **IOS Software**, then select the latest IOS release.

Download the image you identified in Step 1.

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 Software Features

- VACL Logging to generate syslog messages for ACL denied IP packets
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.
- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).

- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Support for the Virtual Router Redundancy Protocol (VRRP) for IPv4, which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.
- Support for IPv4 and IPv6 Gateway Load Balancing Protocol (GLBP) for automatic router backup for IP hosts configured with a single default gateway on a LAN.
- Support for IPv6 features with Catalyst 3750 Metro ES-port specific features, such as hierarchical QoS.
- Support for IPv6 DHCP server, client and relay in a virtual routing and forwarding (VRF) environment with limited VRF flexibility.
- Support for IPv6 Multi-Protocol VRF-CE (also referred to as VRF-Lite).
- Support for Layer 2 protocol tunneling for Link Layer Discovery Protocol (LLDP) traffic.

Minimum Cisco IOS Release for Major Features

Note Features not included in the table are available in all releases. You can see a list of features from the first release: http://www.cisco.com/en/US/docs/switches/metro/catalyst3750m/software/release/12.1_14_ax/configuration/guide/swintro.html

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

Feature	Minimum Cisco IOS Release Required
VACL logging	12.2(58)SE1
Call Home support	12.2(58)SE1
IP/IF MIBs for IPv6	12.2(58)SE1
NTPv4 over IPv6	12.2(58)SE1
DHCPv6 bulk lease query and DHCPv6 relay source configuration	12.2(58)SE1
RADIUS, TACACS+, and SSH/SCP over IPv6	12.2(58)SE1
VRRP version 4 support	12.2(58)SE1
GLBP for IPv4 and IPv6 with VRF-Lite	12.2(58)SE1
IPv6 unicast routing in VRF-Lite	12.2(58)SE1
Support for IPv6 features with ES-port specific features	12.2(58)SE1
VRF-aware IPv6 DHCP server and client support	12.2(58)SE1
802.1Q LLDP tunneling	12.2(58)SE1
Configuration of an alternate MTU value for specific interfaces	12.2(55)SE
BFD Protocol on SVIs	12.2(55)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 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
IPv6 QoS trust capability.	12.2(52)SE
EEM 3.2 support.	12.2(52)SE
IP source guard on static hosts.	12.2(52)SE
802.1x User Distribution for deployments with multiple VLANs.	12.2(52)SE
Network Edge Access Topology (NEAT) for changing the port host mode.	12.2(52)SE
SNMPv3 for 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.	12.2(52)SE
DHCP Snooping enhancement to support the circuit-id sub-option.	12.2(52)SE
Connectivity fault management (CFM) Draft 8.1 compliance.	12.2(52)SE
TWAMP standard for measuring round-trip network performance between any two devices that support the protocol.	12.2(52)SE
IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping.	12.2(52)SE
QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.	12.2(52)SE
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. and IPv6 QoS trust.	12.2(52)SE
Multicast VLAN registration (MVR) enhancements.	12.2(52)SE
Shorter REP hello.	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

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

Feature	Minimum Cisco IOS Release Required
Source Specific Multicast (SSM) mapping for multicast applications	12.2(44)SE
Support for the *, *ip-address*, **interface** *interface-id,* and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command	12.2(44)SE
Flex Link Multicast Fast Convergence	12.2(44)SE
IEEE 802.1x readiness check	12.2(44)SE
Configurable control-plane queue assignment	12.2(44)SE
Prioritization of management traffic	12.2(44)SE
/31 bit mask support for multicast traffic	12.2(44)SE
Configuration replacement and rollback	12.2(40)SE
Embedded event manager (EEM)	12.2(40)SE
Internet Group Management Protocol (IGMP) Helper	12.2(40)SE
IP Service Level Agreements (IP SLAs) support	12.2(40)SE
IP SLAs EOT	12.2(40)SE
IP SLAs for Metro Ethernet using IEEE 802.1ag Ethernet operation, administration, and maintenance (OAM)	12.2(40)SE
Multiprotocol label-switching (MPLS) OAM	12.2(40)SE
Multicast virtual routing and forwarding (VRF) lite	12.2(40)SE
Support for the SSM PIM protocol	12.2(40)SE
Support for the Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE
Support for Resilient Ethernet Protocol (REP)	12.2(40)SE
Ethernet OAM MPLS	12.2(37)SE
ELMI-CE	12.2(37)SE
LLDP and LLDP-MED	12.2(37)SE
Port security on a PVLAN host	12.2(37)SE
VLAN Flex Links load balancing	12.2(37)SE
MVR over trunk port (MVRoT) support	12.2(35)SE1
Hierarchical QoS on ES EtherChannels	12.2(35)SE1
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

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

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

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

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, ARP and RARP packets greater than 2016 bytes are dropped by the switch. 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 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)

- 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. (CSCtf77937)

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

- 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)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

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)

- If you configure two or more connected REP segments to send segment topology change notices (STCNs) by entering the **rep stcn segment** *segment-id* interface configuration command on REP interfaces, when segments inject messages simultaneously, an STCN loop occurs, and CPU usage can increase to 99 percent for 1 to 2 minutes before recovering.

  The workaround is to avoid configuring multiple STCNs in connected segments. This is a misconfiguration. (CSCth18662)

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.

  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)

- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

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 Release12.1(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

- CSCtg98453

  When you make port security changes on an interface, such as configuring aging time, violations, or aging type, error messages and tracebacks might appear.

  There is no workaround.

- CSCtl32991

  Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue.

Note This does not occur when packets are routed through the switch to another destination.

  There is no workaround.

- CSCtl60247

  When a switch running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

- CSCtl81217

  When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, if the switch reloads, the interface loses some RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.

  There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:

  ip rip authentication mode

  ip rip key-chain

Resolved Caveats

- Caveats Resolved in Cisco IOS Release 12.2(55)SE4, page 24

Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- CSCtj83964

  On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.

  The workaround is to enter the **clear ip route** privileged EXEC command or reconfigure PIM and SSM after a reload.

- CSCtl51859

  Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.

  The workaround is to disable IPv6 MLD snooping on the switch.

Caveats Resolved in Cisco IOS Release 12.2(58)SE2

- CSCtq01926

  When you configure a port to be in a dynamic VLAN by entering the **switchport access vlan dynamic** interface configuration command on it, the switch might reload when it processes ARP requests on the port.

  The workaround is to configure static VLANs for these ports.

Caveats Resolved in Cisco IOS Release 12.2(58)SE1

- CSCtg00542

  A Link Aggregation Control Protocol (LACP) bundle takes up to 70 seconds to form when NetFlow sampling is enabled.

  The workaround is to disable NetFlow sampling.

- CSCtg11547

  When you configure a switch to send messages to a syslog server in a VPN Routing and Forwarding (VRF) instance, the messages are not sent to the server.

  The workaround is to remove the VRF configuration.

- CSCtg71149

  When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, indicated by the appearance of `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.

  The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

  - Enter the **shutdown** interface configuration command on each member port.
  - Enter the **shutdown** command on the port-channel interface.

  - Enter the **no shutdown** command on each member port.
  - Enter the **no shutdown** command on the port-channel interface.

- CSCth97324

  When you are configuring 802.1ad on an EtherChannel interface, the **ethernet dot1ad isolate** interface configuration command is visible and available. However, the **isolate** keyword is not supported on the Catalyst 3750 Metro switch. If you enter the **ethernet dot1ad isolate** command on an EtherChannel, the EtherChannel becomes inactive, and strange spanning tree behavior can occur.

  Do not enter the **isolate** keyword on a Catalyst 3750 Metro EtherChannel. The workaround, if you do enter the **isolate** keyword, is to restart the switch.

- CSCti26354

  When a switch running Cisco IOS Release 12.2(53)SE, 12.2(54)SE, or 12.2(55)SE is connected to another switch through a 1000BASE-EX SFP (GLC-EX-SMD) module port, and the link is error disabled, this message appears:

  ```
  %PHY-4-SFP_NOT_SUPPORTED: The SFP in Gi0/1 is not supported
  ```

  There is no workaround.

- CSCti26743

  When you configure an interface that is connected to a customer edge device as an 802.1ad S-UNI port, by default Layer 2 PDUs should be tunneled through the 802.1ad service provider cloud on the S-UNI port configured on the provider edge device. On a Catalyst 3750 Metro switch, LLDP, STP, and other Layer 2 control protocol traffic is correctly tunneled, but end-to-end tunneling is not working for CDP.

  On an 802.1ad S-UNI port connected to a customer port, CDP is automatically disabled to prevent service-provider CDP packets from being propagated to the customer domain. The workaround is to use the command line interface to explicitly enable CDP on the 802.1ad S-UNI port to allow end-to-end tunneling to work correctly. The problem with the workaround is that the customer edge device recognizes the remote customer device as a neighbor, but will also recognize the directly connected provider edge device as a neighbor, which is not desirable when end-to-end tunneling is configured.

- CSCth79300

  When an access control list (ACL) that permits only bidirectional forwarding detection (BFD) and border gateway protocol (BGP) packets is applied to an interface on a switch running Cisco IOS Release 12.2(54)SE, the BFD session goes down but the BGP peer stays up.

  The workaround is to remove the ACL from the interface.

- CSCti24844

  When you apply hierarchical policy-maps to multiple child policy-maps that have the same names and different bandwidth allocations, the **show policy-map interface** interface configuration command output is not correct, although the actual traffic rate conforms to the configuration.

  The workaround is to configure different names for policy-maps that have identical classes.

- CSCti78365

  The config.text.backup file is present after the switch is restored to the factory defaults.

  There is no workaround.

- CSCti95834

When you enter the **ipv6 traffic-filter** interface configuration command, it might not filter traffic as expected, and it might allow traffic to pass through.

There is no workaround.

- CSCtj03875

  When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.

  There is no workaround.

- CSCtj75471

  When a spanning-tree bridge protocol data unit (BPDU) is received on an 802.1Q trunk port and has a VLAN ID is greater than or equal to 4095, the spanning-tree lookup process fails.

  There is no workaround.

- CSCtj88307

  When you enter the **default interface**, **switchport**, or **no switchport** interface configuration command on the switch, this message appears: *EMAC phy access error, port 0, retrying.....*

  There is no workaround.

- CSCtk11275

  On a switch running Cisco IOS Release 12.2(55)SE with the **parser config cache interface** global configuration command in the configuration, when you use the CISCO-MAC-NOTIFICATION-MIB to enable the SNMP MAC address notification trap, the trap is enabled, but the trap setting does not appear in the switch configuration.

  The workaround is to remove the **parser config cache interface** command from the configuration.

- CSCtk15855

  When packets that should be forwarded through the default route in an MPLS network are switched in software, *ADJ Failed* appears in the default route adjacency field of the **show platform ip unicast fail adjacency** command output.

  There is no workaround.

- CSCtk76719

  A switch running Cisco IOS Release 12.2(55)SE that has oversubscribed or congested Resilient Ethernet Protocol (REP) links might experience REP instabilities and display this error message:

  ```
  %REP-4-LINKSTATUS: GigabitEthernet0/12 (segment 1) is non-operational due to neighbor
  not responding
  ```

  There is no workaround.

- CSCtl42740

  When 802.1x MAC authentication bypass with multidomain authentication and critical VLAN are enabled on an interface on a switch running Cisco IOS Release 12.2(53)SE or later, if the switch loses connectivity with the AAA server, the switch might experience high CPU usage and show these messages:

  ```
  AUTH-EVENT (Gi0/15) Received clear security violation
  AUTH-EVENT (Gi0/15) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on port
  GigabitEthernet0/15
  ```

  There is no workaround.

- CSCtl80678

  The port manager callback might cause more than 90% CPU usage for up to 20 minutes under these conditions:

  - Link comes up simultaneously on multiple dot1q trunk ports.
  - VLAN Trunking Protocol (VTP) pruning is enabled.

  The workaround is to disable VTP pruning.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCto62631

  A switch running Cisco IOS Release 12.2(58)SE might reload if:

  - SSH version 2 is configured on the switch, and
  - a customized login banner was configured by using the **banner login** *message* global configuration command

  Use one of these workarounds:

  - Disable the login banner by entering the **no login banner** command.
  - Disable SSH on the switch.
  - Downgrade to a software version prior to Cisco IOS Release 12.2(58)SE.

Documentation Updates

Note The “Supported MIBs” appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

- Updates to the System Message Guide, page 28
- Update to the Hardware Installation Guide, page 29

Updates to the System Message Guide

New System Messages

Error Message `IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]`

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message `AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]`

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars]s is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Modified System Messages

Error Message `AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]`

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message `AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])`

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Deleted System Messages

Error Message `IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST`

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

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

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

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:
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.