Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switches, Cisco IOS Release 12.2(60)EZ and Later

Last Updated: December 2017

Cisco IOS Release 12.2(60)EZ and later releases run on the Cisco ME 3400E and ME 3400 Series Ethernet Access switches.

These release notes include important information about Cisco IOS Release 12.2(60)EZ and later, and any limitations, restrictions, and caveats that apply to the release. 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 5.
- If you are upgrading to a new release or different image, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

For the complete list of Cisco ME 3400E and ME 3400 switch documentation, see the "Related Documentation" section on page 43.

You can download the switch software from this site (registered Cisco.com users with a login password):

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

Cisco Systems, Inc.
www.cisco.com

Contents

Hardware Support

Table 1 Supported Hardware

Device	Description	Supported by Minimum Cisco IOS Release
ME 3400E-24TS-M	24 10/100 ports and 2 dual-purpose ports; supports removable AC- and DC-power supplies.	Cisco IOS Release 12.2(44)EY
ME 3400EG-12CS-M	12 dual-purpose ports and 4 SFP module slots; supports removable AC- and DC-power supplies.	Cisco IOS Release 12.2(44)EY
ME 3400EG-2CS-A	2 dual-purpose ports and 2 SFP module slots, AC-power input.	Cisco IOS Release 12.2(44)EY
ME 3400-24FS-A	24 100BASE-FX SFP module ports and 2 Gigabit Ethernet SFP module ports, AC power	Cisco IOS Release 12.2(40)SE
ME 3400G-2CS	2 dual-purpose ports and 2 SFP-only module ports, AC power	Cisco IOS Release 12.2(35)SE1
ME-3400G-12CS-A	12 dual-purpose ports and 4 SFP-only module ports	Cisco IOS Release 12.2(25)SEG1
ME-3400G-12CS-D	12 dual-purpose ports and 4 SFP-only module ports	Cisco IOS Release 12.2(25)SEG1
ME-3400-24TS-A	24 10/100 ports and 2 SFP module slots, AC power	Cisco IOS Release 12.2(25)EX
ME-3400-24TS-D	24 10/100 ports and 2 SFP module slots, DC power	Cisco IOS Release 12.2(25)EX

Table 1 Supported Hardware (continued)

Device	Description	Supported by Minimum Cisco IOS Release
SFP modules ME 3400	1000BASE-T, -BX, -SX, -LX/LH, -ZX 100BASE-BX, FX, -LX Coarse wavelength-division multiplexing (CWDM)	Cisco IOS Release 12.2(25)EX
	Digital optical monitoring (DOM) support for GLC-BX, CWDM and DWDM SFPs	Cisco IOS Release 12.2(44)SE
	100BASE-EX, 100BASE-ZX 1000BASE-LX/LH MMF and SMF 1000BASE-SX MMF DOM support for GLC-ZX-SM SFP, 1000BASE-LX/LH, and 1000BASE-SX	Cisco IOS Release 12.2(46)SE
	DOM support for 1000BASE-BX Additional DWDM SFPs qualification	Cisco IOS Release 12.2(50)SE
	1000BASE-BX-DA-I, 1000BASE-BX-40U/D, 1000BASE-BX-80D/U	Cisco IOS Release 12.2(60)EZ4
	GLC-LX-NID-0	Cisco IOS Releas7e 12.2(60)EZ7
For a complete list of ME 3400 supported SFPs and part numbers, see the ME 3400 data sheet at: http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps6580/product_data_sheet0900aecd8034fef3.html		
SFP modules ME 3400E	1000BASE-BX10, -SX, -LX/LH, -ZX 100BASE -BX10, -EX, -FX (GLC-FE-100FX only), -LX10, -ZX 1000BASE-T and 10/100/100BASE-T—Category 5,6 (SFP-only ports; not supported on dual-purpose ports) Coarse wavelength-division multiplexing (CWDM) Dense wavelength-division multiplexing (DWDM) Digital optical monitoring (DOM) support for SFP-GE-S, SFP-GE-L, 1000BASE-BX10, 1000BASE-ZX, CWDM and DWDM SFPs **Note** See the hardware installation guide for SFP model numbers.	Cisco IOS Release 12.2(44)EY
	Additional DWDM SFPs qualification	Cisco IOS Release 12.2(50)SE
	1000BASE-BX-DA-I, 1000BASE-BX-40U/D, 1000BASE-BX-80D/U	Cisco IOS Release 12.2(60)EZ4
	GLC-LX-NID-0	Cisco IOS Release 12.2(60)EZ7
	Cisco NID Smart SSFP	Cisco IOS Release 12.2(60)EZ7

Note DOM status helps monitor optical transceivers in the system and generates system log every 600 seconds (10 minutes). This update period is not configurable, and hence the reporting of changes in the status may lag behind the actual status changes due to the update rate.

Table 1 Supported Hardware (continued)

Device	Description	Supported by Minimum Cisco IOS Release
For a complete list of ME 3400E supported SFPs and part numbers, see the ME 3400E data sheet at: http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps9637/data_sheet_c78-495220.html		
Cable	Catalyst 3560 SFP interconnect cable	Cisco IOS Release 12.2(25)EX

Upgrading the Switch Software

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. The second line of the display shows the version.

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 filenames for this software release.

Note Effective with Cisco IOS Release 12.2(60)EZ, the ME 3400 metro base image is supported on the Cisco ME 3400E switch.

Table 2 Cisco IOS Software Image Files

Filename	Description
me340x-metrobasek9-tar.122-60.EZ4.tar	Cisco ME 3400 metro base cryptographic image with Kerberos, Secure Shell (SSH), and basic Metro Ethernet features.
me340x-metroaccessk9-tar.122-60.EZ4.tar	Cisco ME 3400E and ME 3400 metro access cryptographic image with Kerberos, SSH, and Layer 2 + Metro Ethernet features.
me340x-metroipaccess9-tar.122-60.EZ4.tar	Cisco ME 3400E and ME 3400 metro IP access cryptographic image with Kerberos, SSH, Layer 2+, and full Layer 3 routing Metro Ethernet features.

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.

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* at this URL:

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

Upgrading a Switch

This procedure is for copying the combined 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.

Note For downloading software, we recommend that you connect to the TFTP server through a network node interface (NNI). If you want to connect to the server through a user network interface (UNI), see the "Troubleshooting" chapter of the software configuration guide for methods for enabling ping capability on UNIs.

To download software, follow these steps:

Step 1 Use Table 2 on page 5 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, refer to Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

Note By default, ping is supported on network node interfaces (NNIs), but you cannot ping from a user network interface (UNI) because the control-plane security feature drops ICMP response packets received on UNIs. See the "Troubleshooting" chapter of the software configuration guide for methods for pinging from the switch to a host connected to a UNI.

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

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 entering this privileged EXEC command:

```
Switch# 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 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 198.51.100.1 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite

tftp://198.51.100.1/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

For 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 these methods:

- Using the CLI-based setup program, as described in the switch hardware installation guide.
- Using the DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Software Features

The following features are introduced on the Cisco ME 3400E and ME 3400 switches for Cisco IOS Release 12.2(60)EZ:

- IPv6 QoS features
  - Class-default Classification for Ingress—Support is added for classifying IPv6 traffic into the default class of a policy map. Policy maps specify which traffic to act on and what actions to take. All ingress and egress traffic that fail to meet the matching criteria of a traffic class belongs to the default class.
  - DSCP Classification for Both IPv4 and IPv6 for Ingress—Support is added for the **match dscp** command. The **match dscp** command classifies both IPv4 and IPv6 traffic based on DSCP value.
  - IPv6-ACL Based Classification (SA/DA, v6 DSCP) for Ingress—Support is added for matching IPv6 traffic based on source/destination address, IPv6 DSCP, and Layer 4 source/destination port by defining ACLs and matching on the ACL.
  - IPv6 DSCP Marking (Set and Police) for Ingress—Support is added for marking and policing of IPv6 traffic.
  - Port-based QoS MIB—Support is added for the enhanced match capabilities to match IPv6 traffic based on DSCP value.
  - VLAN Classification (Per-Port, Per-LAN Policies) for Ingress—All IPv6 QoS classification and marking features can be configured in the child-policy of a per-port, per-VLAN policy.

  For more information about the IPv6 QoS features on the Cisco ME 3400E, refer to the Configuring IPv6 QoS section of the *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide, Release 12.2(60)EZ* at

  http://www.cisco.com/en/US/products/ps9637/products_installation_and_configuration_guides_list.html

  For more information about the IPv6 QoS features on the Cisco ME 3400, refer to the Configuring IPv6 QoS section of the *Cisco ME 3400 Ethernet Access Switch Software Configuration Guide, Release 12.2(60)EZ* at

  http://www.cisco.com/en/US/products/ps6580/products_installation_and_configuration_guides_list.html

- IPv6 IS-IS—This feature extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

  For more information about this feature on the Cisco ME 3400E, refer to Configuring IS-IS for IPv6 in the Configuring IPv6 Unicast Routing section of the *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide, Release 12.2(60)EZ* at

  http://www.cisco.com/en/US/products/ps9637/products_installation_and_configuration_guides_list.html

  For more information about this feature on the Cisco ME 3400, refer to Configuring IS-IS for IPv6 in the Configuring IPv6 Unicast Routing section of the *Cisco ME 3400 Ethernet Access Switch Software Configuration Guide, Release 12.2(60)EZ* at

  http://www.cisco.com/en/US/products/ps6580/products_installation_and_configuration_guides_list.html

- ME-3400-E Metro Base Image
  - me340x-metrobasek9-mz.122-60.EZ
  - me340x-metroaccessk9-mz.122-60.EZ
  - me340x-metroipaccessk9-mz.122-60.EZ
  - me340x-metrobasek9-tar.122-60.EZ
  - me340x-metroaccessk9-tar.122-60.EZ
  - me340x-metroipaccessk9-tar.122-60.EZ

Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release (after the first release) required to support the features of the Cisco ME 3400E and ME 3400 switch. Features not listed are supported in all releases.

Note The first release for the Cisco ME3400E switch was 12.2(44)EY, and it included all ME 3400 features through release 12.2(44)SE.

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
IPv6 QoS features	12.2(60)EZ
IPv6 IS-IS	12.2(60)EZ
REP 2 Edge No-Neighbor Ports on Single Node	12.2(58)EZ
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
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
Support for 802.1ad split horizon (ME 3400E).	12.2(55)SE
QoS classification and marking DEI bit in an IEEE 802.1ad frame (ME 3400E)	12.2(55)SE
Support for the IEEE 802.1ad standard (ME 3400E).	12.2(54)SE

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
CFM support on customer VLANs (C-VLANs).	12.2(54)SE
IEEE CFM MIB support.	12.2(54)SE
Ingress QoS classification enhancements	12.2(53)SE
Support for ingress QoS classification on QinQ-based ports (ME 3400E).	12.2(53)SE
Support for EEM 3.2	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.	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
Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3).	12.2(52)SE
Support for including a hostname in the option 12 field of DHCPDISCOVER packets.	12.2(52)SE
DHCP snooping circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE
Connectivity fault management (CFM) Draft 8.1 compliance.	12.2(52)SE
Support for the TWAMP standard for measuring round-trip network performance between two devices.	12.2(52)SE
Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, HTTP, and 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
Multicast VLAN registration (MVR) enhancements.	12.2(52)SE
Resilient Ethernet Protocol (REP) hello link status layer (LSL) age timer configurable from 120 to 10000 ms in 40-ms intervals.	12.2(52)SE
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE
IPv6 routing support (metro IP access image only)	12.2(50)SE
IPv6 ACLs (metro IP access image only)	12.2(50)SE
BFD (metro IP access image only)	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 (metro access image only on ME 3400)	12.2(50)SE
RADIUS server load balancing	12.2(50)SE
IP source guard in metro base image (ME 3400)	12.2(50)SE
Dynamic ARP inspection in metro base image (ME 3400)	12.2(50)SE
EOT and IP SLAs EOT static route support	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
REP counter and timer enhancements	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
HSRPv2 (metro IP access image only)	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
DHCP server port-based address allocation	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
DHCP-based autoconfiguration and image update	12.2(44)SE
Configurable small-frame arrival threshold	12.2(44)SE
Source Specific Multicast (SSM) mapping for multicast applications	12.2(44)SE
Support for the *, *ip-address*, **interface** *interface-id,* and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command	12.2(44)SE
Flex Link Multicast Fast Convergence	12.2(44)SE
IEEE 802.1x readiness check	12.2(44)SE
Configurable control-plane queue assignment	12.2(44)SE
Configurable control plane security (support for ENIs)	12.2(44)SE
/31 bit mask support for multicast traffic	12.2(44)SE
Configuration rollback and replacement	12.2(40)SE
EEM (metro IP access image only) **Note** EEM support was added to the metro access image in 12.2(44)SE	12.2(40)SE
IGMP Helper (metro IP access image only)	12.2(40)SE
IP SLAs support (metro IP access and metro access images only)	12.2(40)SE
IP SLAs enhanced object tracking (metro IP access and metro access images only)	12.2(40)SE
IP SLAs for Ethernet OAM (metro IP access image only)	12.2(40)SE
Multicast VRF Lite (metro IP access image only)	12.2(40)SE
SSM PIM (metro IP access image only)	12.2(40)SE
REP (metro IP access and metro access images only)	12.2(40)SE
LLDP-MED location TLV (metro IP access and metro access images only)	12.2(40)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
Support for Multicast VLAN Registration (MVR) over trunk ports	12.2(35)SE1
Enhanced object tracking for HSRP (metro IP access image only)	12.2(35)SE1
Ethernet OAM IEEE 802.3ah protocol (metro IP access and metro access images only)	12.2(35)SE1
Ethernet OAM CFM (IEEE 802.1ag) and E-LMI (metro IP access and metro access images only)	12.2(25)SEG
Per port per VLAN QoS (metro IP access and metro access images only)	12.2(25)SEG
Support for all OSPF network types (metro IP access only)	12.2(25)SEG

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
Layer 2 protocol tunneling on trunks (metro IP access and metro access images only)	12.2(25)SEG
IS-IS protocol (metro IP access only)	12.2(25)SEG
NNIs on all ports (metro IP access image only)	12.2(25)SEG
DHCP server	12.2(25)SEG
DHCP Option-82 configurable remote ID and circuit ID	12.2(25)SEG
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEG
Nonstop forwarding (NSF) awareness (metro IP access image only)	12.2(25)SEG
Secure Copy Protocol	12.2(25)SEG
Flex Links sub-100-ms convergence; preemptive changeover (metro IP access and metro access images)	12.2(25)SEG
Link-state tracking (trunk failover) (metro IP access and metro access images only)	12.2(25)SEG

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations, 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

- The BFD session with the neighbor flaps when there is close to 100 percent bidirectional line- rate traffic sent through the physical links connecting the neighbors. This happens only on the sessions with Layer 3 BFD neighboring switches connected through a Layer 2 intermediate switch.

  The workaround is to make sure that there is no 100 percent bidirectional unknown traffic flowing through the intermediate Layer 2 switch in the same links that connect Layer 3 switches. An alternate workaround is to always directly the Layer 3 switches when BFD is running. (CSCsu94835)

- 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 the **permit** ACL entry with the log option on interfaces participating in BFD. (CSCtf31731)

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 ME 3400 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)‘

Configuration

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244)

- 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 and CSCdz11708)

- The DHCP snooping binding database is not written to flash memory 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 the 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 manually removed 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 was 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 or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)
- 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 are 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 you entered the command.

  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 on 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 on that specific interface. (CSCee93822)
- 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 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)
- When an ME 3400 port is connected to an ME 3400E port, if one port is configured to 10 Mb/s and the other port is configured to 100 Mb/s (either full or half duplex), the 10 Mb/s port state appears as up/up and the 100 Mb/s port appears as down/down. This connection is a misconfiguration because the speed and duplex do not match.

  The workaround is to correct the misconfiguration. (CSCtg53462)

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 (Cisco ME 3400E only)

IP

- The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out.

  The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

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.

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)

Multicasting

- The switch does not support tunnel interfaces, including DVMRP and PIM tunneling.
- 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 group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port.

  There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by 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 reachability to directly connected clients, if any, in the VLAN.

  The workaround is to not apply a router ACL set 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)

- 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 IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

REP

- 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 1000 milliseconds (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 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 routed traffic.
- A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message 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)

QoS

- When you use the **bandwidth** policy-map class command to configure more than one class in a policy map for Class-based Weighted Fair Queuing (CBWFQ), and the committed information rate (CIR) bandwidth for any of the classes is less than 2 percent of the interface rate, the CBWFQ classes in the policy may not receive the configured CIR bandwidths.

  There is no workaround, but it is unlikely that a CBWFQ class would be configured with such a low CIR bandwidth. (CSCsb98219)

- When several per-port, per-VLAN parent policies are attached to the input of one or more interfaces and a child policy of these parent policies is modified, the parent policies are detached from the interfaces and reattached during the process. Because the modified policy is large, the TCAM entries are being used up, and the attached policies should be removed. However, some of the parent

policies are not removed from the interface, and the TCAM entries are cleared. If you save the configuration and reload the switch, the policies are detached, but the TCAM is full, and you cannot attach other policies.

This error message appears:

```
QOSMGR-4-QOS_TCAM_RESOURCE_EXCEED_MAX: Exceeded a maximum of QoS TCAM resources
```

The workaround is to manually detach the policy maps from all the interfaces by entering the **no service-policy input** *policy-map-name* interface configuration command on each interface. (CSCsk58435)

- When CPU protection is disabled, you can configure 64 policers per port on most switches. However, on Cisco ME 3400EG-12CS and Cisco ME 3400G-12CS switches, due to hardware limitations, you can attach 64 per-port, per-VLAN policers to a maximum of 6 ports. If you attempt to attach more than 6 per-port, per-VLAN 64-policer policy maps, the attachment fails.

  There is no workaround. (CSCsv21416)

SPAN and RSPAN

- The egress SPAN data rate might degrade when multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following 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 egress spanned. If multicast routing is disabled, egress SPAN is not degraded.

  There is no workaround. If possible, disable 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-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned.

  There is no workaround. (CSCeb23352)

- 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)

- Cisco Discovery Protocol (CDP) and Port Aggregation Protocol (PAgP) packets received by network node interfaces (NNIs) 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 local SPAN. (CSCed24036)

Trunking

- 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 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)

VLAN

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

  The workaround is to not configure more than the recommended number of VLANs and 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 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

- When you upgrade the switch software to Cisco IOS release 12.2(50)SE or higher and autonegotiation is enabled on a Gigabit SFP fiber switch port (the default), but disabled on the link partner port, the switch port interface can show a state of down/down while the link partner shows up/up. This is expected behavior.

  The workaround is to either enable autonegotiation on the link partner port or enter the **speed nonegotiate** interface command on the SFP port.

Open Caveats

The following sections provide information about open caveats:

Open Caveats in Cisco IOS Release 12.2(60)EZ12

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ11

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ10

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ9

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ8

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ7

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ6

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ5

There are no open caveats in this release.

Open Caveats in Cisco IOS Release 12.2(60)EZ3

- **CSCuf73492**

Basic Description

Invalid per-port, per-VLAN policy-map is not rejected on the dot1q-tunnel port.

Symptom:

Invalid per-port, per-VLAN (PPPV) policy attachment is not rejected on the dot1q tunnel port. This leads to the removal of the policy-map, and also displays hpm_main_process traceback messages upon reload.

Conditions:

This issue occurs only when the same S-VLAN has layer 2 and layer 3 child policies across the Cisco ME 3400E and ME 3400 switches. That is, there is another PPPV policy-map on another trunk port on the switch that matches the same S-VLAN being tunneled on the dot1q tunnel port. Additionally, the PPPV has a child-policy whose protocol does not match with the protocol of the child policy on the dot1q tunnel port.

The problem is specific to dot1q tunnel ports. Policy attachment is rejected as expected on trunk ports.

Workaround:

There is no workaround.

- **CSCug43707**

  Basic Description

  Dynamic class-map modification displays an invalid error message.

  Symptom:

  Dynamic class-map displays an error message.

  Conditions:

  This issue occurs when the class-map is modified on the fly. The error message generated here is inconsistent.

  Workaround:

  Remove and re-attach the service policy-map.

- **CSCuh35495**

  Basic Description

  An invalid error message is displayed when a new class is attached to a child policy that contains class-default.

  Symptom:

  Upon dynamic modification, an invalid error message is displayed when the new class is attached to the child-policy containing the class-default.

  Conditions:

  This issue occurs when the policy-map contains only the policy with class-default.

  Workaround:

  There is no workaround.

- **CSCuj49773**

  Basic Description

  Policy-map gets detached and returns error message after a reload.

Symptom:

Policy-map gets detached and returns error message after a reload when configured with 64 policer.

Conditions:

This issue occurs when the policy-map is configured with 64 policers on each trunk port and the switch is reloaded.

Workaround:

Re-attach the policy-map after reloading the switch.

Open Caveats in Cisco IOS Release 12.2(60)EZ2

- **CSCuf30094**

  Basic Description

  Two SFP Ports have the same entPhysicalName.

  Symptom:

  The EntityMIB response displays the same entPhysicalName for two SFP ports, where entPhysicalName is unique.

  Conditions:

  This issue occurs under normal conditions.

  Workaround:

  There is no workaround.

- **CSCuf73492**

  Basic Description

  Invalid per-port, per-VLAN policy-map is not rejected on the dot1q-tunnel port.

  Symptom:

  Invalid per-port, per-VLAN (PPPV) policy attachment is not rejected on the dot1q tunnel port. This leads to the removal of the policy-map, and also displays hpm_main_process traceback messages upon reload.

  Conditions:

  This issue occurs only when the same S-VLAN has layer 2 and layer 3 child policies across the Cisco ME 3400E and ME 3400 switches. That is, there is another PPPV policy-map on another trunk port on the switch that matches the same S-VLAN being tunneled on the dot1q tunnel port. Additionally, the PPPV has a child-policy whose protocol does not match with the protocol of the child policy on the dot1q tunnel port.

  The problem is specific to dot1q tunnel ports. Policy attachment is rejected as expected on trunk ports.

  Workaround:

  There is no workaround.

- **CSCug43707**

  Basic Description

  Dynamic class-map modification displays an invalid error message.

Symptom:

Dynamic class-map displays an error message.

Conditions:

This issue occurs when the class-map is modified on the fly and this error message is inconsistent.

Workaround:

Remove and re-attach the service policy-map.

- **CSCuh35495**

  Basic Description

  An invalid error message is displayed when a new class is attached to a child policy that contains class-default.

  Symptom:

  Upon dynamic modification, an invalid error message is displayed when the new class is attached to the child-policy containing the class-default.

  Conditions:

  This issue occurs when the policy-map contains only the policy with class-default.

  Workaround:

  There is no workaround.

- **CSCuh59574**

  Basic Description

  Connectivity Fault Management (CFM) Loopback Message (LBM)/Loopback Reply (LBR) does not work on the MIP that is configured with port-type user network interface (UNI) or with enhanced network interface (ENI).

  Symptom:

  The CFM loopback message does not appear on a port-type configured as UNI or ENI.

  Conditions:

  This issue occurs when the port is configured as ENI or UNI.

  Workaround:

  Configure the port as network-to-network interface (NNI).

- **CSCui12155**

  Basic Description

  Abnormal temperature is detected on the bootup metrobase.

  Symptom:

  The Cisco ME 3400E switch displays the following syslog message when the system boots:

  ```
  %PLATFORM_ENV-1-TEMP: Abnormal temperature detected
  ```

  Conditions:

  This issue occurs when the system boots.

  Workaround:

  There is no workaround.

- **CSCuj49773**

Basic Description

Policy-map gets detached and returns error message after a reload.

Symptom:

Policy-map gets detached and returns error message after a reload when configured with 64 policer.

Conditions:

This issue occurs when the policy-map is configured with 64 policers on each trunk port and the switch is reloaded.

Workaround:

Re-attach the policy-map after reloading the switch.

- **CSCuj70503**

  Basic Description

  Found traceback and PPPOE_IA-3-INTERFACE_ERROR for PPPoEIA that is disabled and calls for VLAN.

  Symptom:

  Traceback messages and PPPOE_IA-3-INTERFACE_ERROR are received when PPPoE session calls for the VLAN on which PPPoIA is not enabled.

  Conditions:

  This issue occurs when PPPoE session calls for the VLAN on which PPPoEIA is not enabled.

  Workaround:

  Enable the PPPoEIA for the called VLAN.

Open Caveats in Cisco IOS Release 12.2(60)EZ1

- **CSCuf73492**

  Basic Description

  Invalid per-port, per-vlan policy-map is not rejected on the dot1q-tunnel port.

  Symptom:

  Invalid per-port, per-vlan (PPPV) policy attachment is not rejected on the dot1q tunnel port, causing removal of the policy-map and a display of hpm_main_process traceback messages on reload.

  Conditions:

  This issue occurs only when the same S-VLAN has layer 2 and layer 3 child policies across the Cisco ME 3400E and ME 3400 switches. That is, there is another PPPV policy-map on another trunk port on the switch that matches the same S-VLAN being tunneled on the dot1q tunnel port. Additionally, the PPPV has a child-policy whose protocol does not match with the protocol of the child policy on the dot1q tunnel port.

  The problem is specific to dot1q tunnel ports. Policy attachment is rejected as expected on trunk ports.

  Workaround:

  There is no workaround.

- **CSCug61781**

Basic Description

The **show platform tcam utilization** command shows lesser entries for IPv6 QoS.

Symptom:

The ternary content addressable memory (TCAM) displays lesser entries than defined for IPv6 QoS.

Conditions:

This issue occurs when using IPv6 QoS.

Workaround:

There is no workaround.

- **CSCuh35495**

  Basic Description

  An invalid error message is displayed when a new class is attached to a child policy that contains class-default.

  Symptom:

  Upon dynamic modification, an invalid error message is displayed when the new class is attached to the child-policy containing the class-default.

  Conditions:

  This issue occurs when the policy-map contains only the policy with class-default.

  Workaround:

  There is no workaround.

- **CSCuh59574**

  Basic Description

  Connectivity Fault Management (CFM) Loopback Message (LBM)/Loopback Reply (LBR) does not work on the MIP that is configured with port-type user network interface (UNI) or enhanced network interface (ENI).

  Symptom:

  The CFM loopback message does not appear on a port-type configured as UNI or ENI.

  Conditions:

  This issue occurs when the port is configured as ENI or UNI.

  Workaround:

  Configure the port as network-to-network interface (NNI).

- **CSCuh69964**

  Basic Description

  The Point-to-Point Protocol over Ethernet Intermediate Agent (PPPoEIA) configuration is not removed from the etherchannel interface.

  Symptom:

  The old configuration is applied on the port-channel and on the member interface even after removing the old configuration.

  Conditions:

  This issue occurs when the PPPoEIA configuration is applied on port-channel interface.

Workaround:

To use the same port-channel group with the new configuration, you can do either of the following:

- erase the saved configuration and then reload the device
- undo the command on port-channel
- create a port-channel with a different group number.

Open Caveats in Cisco IOS Release 12.2(60)EZ

- **CSCue13270**

  Basic Description

  show dot1q-tunnel displays traceback.

  Symptom:

  When using the **show dot1q-tunnel** command, the switch displays traceback errors. There is no impact on the show command.

  Conditions:

  This issue occurs when the **show dot1q-tunnel** command is executed.

  Workaround:

  There is no workaround.

- **CSCue78127**

  Basic Description

  Unable to modify child class of a per-port, per-vlan policy dynamically.

  Symptom:

  Adding, deleting, or modifying the class or match statement in the child policy of a per-port, per-vlan hierarchical policy attached to an interface, displays an incorrect error message.

  Conditions:

  This issue occurs when modifications are made dynamically.

  Workaround:

  To modify the child class, first remove the policy-map from the interface.

- **CSCuf51473**

  Basic Description

  Policer QoS marking **set-dot1ad-dei-transmit** command does not take effect.

  Symptom:

  Configuration changes for the QoS do not take effect through the **set-dot1ad-dei-transmit** command.

  Conditions:

  This issue occurs under normal conditions when configuring policer QoS marking action as **set-dot1ad-dei-transmit**.

  Workaround:

  There is no workaround.

- **CSCuf73492**

  Basic Description

  Invalid per-port, per-vlan policy-map is not rejected on the dot1q-tunnel port

  Symptom:

  Invalid per-port, per-vlan (PPPV) policy attachment is not rejected on the dot1q tunnel port, causing removal of the policy-map and a display of hpm_main_process tracebacks on reload.

  Conditions:

  This issue occurs only when the same S-VLAN has layer 2 and layer 3 child policies across the switch.That is, there is another PPPV policy-map on any other trunk port on the switch that matches the same S-VLAN being tunneled on the dot1q tunnel port and has a child-policy whose protocol does not match with the protocol of the child policy being attached on the dot1q tunnel port.

  The problem is specific to dot1q tunnel ports. Policy attachment is rejected as expected on trunk ports.

  Workaround:

  There is no workaround.

- **CSCug06704**

  Basic Description

  IS-ISv6 adjacency are not coming up after copying saved configuration into the running-configuration.

  Symptom:

  IS-ISv6 adjacency are not displayed after copying the start-up configuration to the running-configuration.

  Conditions:

  This issue occurs after copying the start-up configuration to the running-configuration.

  Workaround:

  First disable and then enable the specified IPv6 IS-IS routing process on the interface.

- **CSCug33206**

  Basic Description

  Classification does not work when the source IPv6 address has a short prefix.

  Symptom:

  Class matching on the source IPV6 address does not classify traffic as expected.

  Conditions:

  This issue occurs when the source address is configured with a prefix that specifies only a single octet.

  Workaround:

  Configure the source IPv6 address with a longer prefix of at least three octets.

- **CSCug37426**

  Basic Description

  cportQosClassifiedPkts and cportQosNoChangePkts do not respond to the SNMP query.

  Symptom:

cportQosClassifiedPkts and cportQosNoChangePkts do not respond to the SNMP query.

Conditions:

This issue occurs when the MIB objects—cportQosClassifiedPkts and cportQosNoChangePkts, are queried.

Workaround:

There is no workaround.

Resolved Caveats

The following sections provide information about resolved caveats:

Resolved Caveats in Cisco IOS Release 12.2(60)EZ12

Caveat ID Number	Description
CSCvf01102	Steady memory leak in ARP background/ADJ resolves proc-12.2(60)EZ10

Resolved Caveats in Cisco IOS Release 12.2(60)EZ11

Caveat ID Number	Description
CSCsh15817	UDP socket events are not received by RTR responder process

Resolved Caveats in Cisco IOS Release 12.2(60)EZ10

Identifier	Description
CSCuz87484	Dying Gasp trap is missing sysUpTime.0

Resolved Caveats in Cisco IOS Release 12.2(60)EZ9

Identifier	Description
CSCuv91867	Unwanted MIP created on dot1q tunnel interface
CSCuy53092	Flowcontrol broken in 58.SE and 55.SE3 testing builds
CSCuy76827	IGMP snooping isn't working after a STP change on ME3400 device
CSCux40397	ME3400: ARP layer 2 loops in double tagged VLANs when DAI enabled
CSCuv39991	ME3400E: policy-map not classifying traffic correctly

Resolved Caveats in Cisco IOS Release 12.2(60)EZ8

Identifier	Description
CSCsq41792	Crash at hlfm_find_di_from_pi
CSCut47372	policy-map not classifying traffic correctly
CSCuu24095	Storm control blocks broadcast after storm stops.
CSCum94811	TCP Packet Memory Leak Vulnerability

Resolved Caveats in Cisco IOS Release 12.2(60)EZ7

- CSCur98244—write memory fails with snmp-server host ethernet-cfm configuration.
- CSCus14471—ARP packets crossing STP blocking port.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ6

- CSCtq15993—Fix new compiler build errors in powernet component in flo_gsbu8.
- CSCuq74142—Placeholder bug for upgrading aaa component.
- CSCuq54085—MAC is not learned from ARP with QinQ and DAI enabled.
- CSCuq4335—ME3400E: Dynamic ARP Inspection Denial of Service Vulnerability.
- CSCur21533—ME3400 processes PPPoE packets on stp blocking port and for disabled VLAN.
- CSCuq78428—PPPoE IA enhancement of the command in Global configuration mode.
- CSCtn67508—MA2: Energy-wise phase-2.5 feature commit.

- CSCtb45916—Energy-wise level at global is removed after default interface.
- CSCto94418—Assert at powernet_create_entity_attr().
- CSCug31122—Workaround fix for VTY hung issues.
- CSCtr96848—Switch members crashed at tplus_free_context.
- CSCuo02995—5760 WLC sends only device certificate.
- CSCun7918 —3850: Standby reload with PKI.
- CSCup59764—ME3400: TPLUS memory leak when flapping up-link core interface.
- CSCuj04504—TACACS incremental memory leak when server group is removed and added.
- CSCuj25790 —Get crashed when TACACS server IP is removed and added.
- CSCur37860—ME3400: Revert compilation changes crypto_process_root_cert_s.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ5

- CSCed57404

  Symptom:

  snmp_semaphore may stall the SNMP local engine.

  Conditions:

  This issue occurs after the SNMP server is disabled and re-enabled

  Workaround:

  There is no workaround.

- CSCul37863

  Symptom:

  The bias current value does not display under the DOM parameter.

  Conditions:

  This issue occurs when the a DOM-supported SFP is used. The **show interface Gig** *port_number* **transceiver detail** command does not display the DOM parameter.

  Workaround:

  Thee is no workaround.

- CSCuo48138

  Symptom:

  The NNI capability is available for the Gigabitethernet port. However, when this port is bundled through etherchannel, the NNI capability is lost.

  Conditions:

  This issue occurs when configuring the Ethernet dot1ad NNI for the port channel.

  Workaround:

  Thee is no workaround.

- CSCup01495

  Symptom:

The REP ALT port forwards Layer 2 Protocol Tunneling (L2PT) packet even when the port is in blocking state.

Conditions:

This issue occurs when the **l2protocol-tunnel** command is configured on an NNI port.

Workaround:

Thee is no workaround.

- CSCup10540

  Symptom:

  Packets are dropped when the PPPoEIA is not enabled on the interconnecting links.

  Conditions:

  This issue occurs when the PPPoE is enabled globally so the PPPoE packets are punted to the CPU, but the interface is not configured with the PPPoE, only IA trust is enabled.

  As per the current behavior, the Cisco ME3400 switch does not consider the packet if the PPPoE is not enabled in the interface level although it the interface is trusted. This causes the packets to drop and the PPPoE session not being established.

  Workaround:

  There is no workaround.

- CSCup23223

  Symptom:

  ARP does not work in QinQ setup.

  Conditions:

  This issue occurs when the ARP inspection enabled on the ISP switch. The issue was found on the Cisco ME3400 switch running Cisco IOS Release 12.2(60)EZ4 and later.

  Workaround:

  Configure static ARP entries.

- CSCup75628

  Symptom:

  Enhancement for CE2.0 certification.

  Conditions:

  This enhancement is required for S-UNI and C-UNI.

  Common issues for S-UNI and C-UNI

  1. ELMI–EPL option-2 to forward ELMI packets end-to-end.
  2. PTP-Peer-Delay (PTPD)—Add hooks to handle EPL-option-1 and option-2. Both LLDP and PTPD share the same destination MAC address and behavior is governed commonly. These protocols must be handled separately without any inter-dependency.

  Issues for C-UNI:

  1. Reserved MAC addresses 0B–0F are currently dropped on C-UNI. A provisioning should be made to tunnel these MAC addresses on C-UNI interface.

  Workaround:

  There is no workaround.

- CSCup77439

  Symptom:

  MPLS LDP traffic is not forwarded to other end.

  Conditions:

  This issue occurs when the member of the port channel in the REP ring is removed. This causes MAC to flap. When the system recovers from the MAC flap, traffic does not reaching the other end.

  Workaround:

  Shut down and bring up the port channel.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ4

- **CSCts03820**

  Basic Description

  The auto image install does not work.

  Symptom:

  The auto configuration works fine, but the auto image install fails. The DHCP option 125 and the sub-option 5 does not work.

  Conditions:

  This issue occurs when using IOS release versions 15.0(1)SE or 12.2(55)SE.

  Workaround: There is no workaround.

- **CSCun49283**

  Basic Description

  IPSLA ethernet fluctuations probe incorrect *lossDS* value.

  Symptom:

  Packet loss is seen in the destination to source direction when ethernet fluctuates.

  Conditions:

  This issue occurs when packet loss is seen only in the destination to source direction as the ethernet fluctuates generating multiple probes. Enabling probe debugging can increase the frequency of the issue.

  Workaround: There is no workaround.

- **CSCuh98575**

  Basic Description

  The Cisco ME3400 and ME3400E switch now supports 1000BaseBX 40/80 KM Bi-Di SFP.

  Symptom:

  The Cisco ME3400 and ME3400E switches support 1000BASE-BX-40D, 1000BASE-BX-40U, 1000BASE-BX-80D and 1000BASE-BX-80U SFP as part of enhancements.

  Conditions:

  Support for new BX SFPs.

  Workaround:

There is no workaround.

- **CSCuo11401**

  Basic Description

  There is an increase in the jumbo frame size.

  Symptom:

  The Cisco ME3400 switch now supports upto 9030 bytes of maximum MTU for the jumbo frames, instead of 9000 bytes as an enhancement.

  Conditions:

  This issue occurs under normal conditions.

  Workaround:

  There is no workaround.

- **CSCuo16899**

  Basic Description

  The Cisco ME3400 and ME3400E switch now supports 1000BaseBX-DA-I.

  Symptom:

  The Cisco ME3400 and ME3400E switch now supports 1000BaseBX-DA-I.

  Conditions:

  Support for 1000BaseBX-DA-I.

  Workaround:

  There is no workaround.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ3

- **CSCuf30094**

  Basic Description

  Two SFP ports have the same entPhysicalName.

  Symptom:

  The EntityMIB response displays the same entPhysicalName for two SFP ports, wherein the entPhysicalName should be unique.

  Conditions:

  This issue occurs under normal conditions.

  Workaround:

  There is no workaround.

- **CSCui12155**

  Basic Description

  Abnormal temperature is detected on the bootup metrobase.

  Symptom:

  The Cisco ME 3400E switch displays the following syslog message when the system boots:

  ```
  %PLATFORM_ENV-1-TEMP: Abnormal temperature detected
  ```

Conditions:

This issue occurs when the system boots.

Workaround:

There is no workaround.

- **CSCuj79953**

  Basic Description

  The **logging event spanning-tree** configuration does not show up in the running configuration.

  Symptom:

  The l**ogging event spanning-tree** configuration is not seen in the running configuration.

  Conditions:

  This issue occurs under normal conditions.

  Workaround:

  There is no workaround.

- **CSCuj85382**

  Basic Description:

  The Cisco ME 3400EG switch crashes due to the CFM traceroute cache issue.

  Symptom:

  The Cisco ME 3400EG switch reloads due to the CFM traceroute cache issue.

  Conditions:

  This issue occurs during the following conditions:

  – when the **ethernet cfm traceroute cache** command is used to configure

  – when a local only ethernet traceroute is performed

  Workaround:

  Disable the CFM traceroute cache by removing the **ethernet cfm traceroute cache** configurations.

- **CSCul37552**

  Basic Description:

  The counters increment abnormally when **show policy-map interface** command is used.

  Symptom:

  The counters increment abnormally when **show policy-map interface** command is used.

  Conditions:

  This issue occurs when there is two-way traffic from the IXIA.

  Workaround:

  Reload the box.

- **CSCum57491**

  Basic Description:

  The **ethernet CFM Global** command causes MAC to flap.

  Symptom:

The **ethernet CFM Global** command causes MAC to flap.

Conditions:

This issue occurs when the switch receives the ethernet CFM packet with DST MAC address as CFM address, and receives e-type as unknown ether type, causing the MAC to flap.

Workaround:

There is no workaround.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ2

- **CSCuh69964**

  Basic Description

  The Point-to-Point Protocol over Ethernet Intermediate Agent (PPPoEIA) configuration is not removed from the etherchannel interface.

  Symptom:

  The old configuration is applied on the port-channel and on the member interface even after removing the old configuration.

  Conditions:

  This issue occurs when the PPPoEIA configuration is applied on port-channel interface.

  Workaround:

  To use the same port-channel group with the new configuration, you can do either of the following:

  – erase the saved configuration and then reload the device

  – undo the command on port-channel

  – create a port-channel with a different group number.

- **CSCuh98938**

  Basic Description

  Adding new VLAN to the REP ALT port leaks the frames on port-channel.

  Symptom:

  Adding new VLAN to REP ALT port causes the frame leak on port-channel.

  Conditions:

  This issue occurs when the ALT port is configured on port-channel.

  Workaround:

  Perform shut or no shut of the ALT port.

- **CSCui78772**

  Basic Description

  The ciscoEnvMonFanStatusEntry on the Cisco ME 3400 switch returns duplicate value.

  Symptom:

  SNMP OID ciscoEnvMonFanStatusEntry on the cisco ME 3400 switch returns duplicate value.

  Conditions:

  This issue occurs during poll of the ciscoEnvMonFanStatusEntry OID.

Workaround:

Use the following SNMP view command to exclude particular MIB OID to get poll.

- **snmp-server view testview iso included**
- **snmp-server view testview ciscoEnvMonFanStatusEntry excluded**
- **snmp-server community public view testview RO**

- **CSCui87376**

  Basic Description

  The ciscoEnvMonSupplyStatusDescr OID displays incorrect SNMP response.

  Symptom:

  The envMon MIB OID ciscoEnvMonSupplyStatusDescr displays incorrect information.

  Conditions:

  This issue occurs during poll of the ciscoEnvMonSupplyStatusDescr SNMP OID.

  Workaround:

  There is no workaround.

- **CSCui90256**

  Basic Description

  Unable to configure QOS policy on the Cisco ME 3400 and the Cisco ME 3400E switches.

  Symptom:

  Unable to apply service-policy to the interface.

  Conditions:

  This issue occurs under normal conditions.

  Workaround:

  There is no workaround.

- **CSCuj19867**

  Basic Description

  PPPoE IA drop PPPoE discovery packets.

  Symptom:

  The PPPoE discovery packets are getting dropped on PPPoEIA device.

  Conditions:

  This issue occurs when the PPPoEIA is enabled globally, under the interface, and then the PPPoE session is called.

  Workaround:

  Disable and enable PPPoEIA globally.

- **CSCuj50163**

  Basic Description

  The switch stops responding after the system is reloaded with 64 aggregate policer.

  Symptom:

  The Cisco ME3400 switch does not respond after system reloads with 64 aggregate policer.

Conditions:

This issue occurs when 64 aggregate policer is created, along with do write memory and the switch is reloaded.

Workaround:

There is no workaround.

- **CSCui98241**

  Basic Description

  The Cisco ME3400 switch generates IGMP leave packets for every inactive MVR group.

  Symptom:

  IGMP burst occurs in MVR dynamic mode when the Cisco ME3400 switch generates IGMP leave packets for every inactive MVR group addresses as a response to IGMP general query.

  Conditions:

  This issue occurs due MVR dynamic mode.

  Workaround:

  Downgrade to 12.2.(55)SE.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ1

- **CSCue13270**

  Basic Description

  The **show dot1q-tunnel** command displays traceback messages.

  Symptom:

  When using the **show dot1q-tunnel** command, the Cisco ME 3400E and ME 3400 switches display traceback error messages. There is no impact on the show command.

  Conditions:

  This issue occurs when the **show dot1q-tunnel** command is executed.

  Workaround:

  There is no workaround.

- **CSCue78127**

  Basic Description

  Unable to modify child class of a per-port, per-vlan policy dynamically.

  Symptom:

  Adding, deleting, or modifying the class or match statement in the child policy of a per-port, per-vlan hierarchical policy attached to an interface, displays an incorrect error message.

  Conditions:

  This issue occurs when modifications are made dynamically.

  Workaround:

  To modify the child class, first remove the policy-map from the interface.

- **CSCuf51473**

Basic Description

Policer QoS marking using the **set-dot1ad-dei-transmit** command does not take effect.

Symptom:

Configuration changes for the QoS do not take effect when using the **set-dot1ad-dei-transmit** command.

Conditions:

This issue occurs under normal conditions when configuring policer QoS marking action as set-dot1ad-dei-transmit.

Workaround:

There is no workaround.

- **CSCug33206**

  Basic Description

  Classification does not work when the source IPv6 address has a short prefix.

  Symptom:

  Class matching on the source IPV6 address does not classify traffic as expected.

  Conditions:

  This issue occurs when the source address is configured with a prefix that specifies only a single octet.

  Workaround:

  Configure the source IPv6 address with a longer prefix of at least three octets.

Resolved Caveats in Cisco IOS Release 12.2(60)EZ

- **CSCud06955**

  Basic Description

  PPPoE IA: Getting Traceback and PPPOE_IA-3-GLOBAL_ERROR message with PACL.

  Symptom:

  Traceback errors are displayed when PACL is configured.

  Conditions:

  This issue occurs when PACL is configured and the PPPoE session is called.

  Workaround:

  There is no workaround.

- **CSCud31166**

  Basic Description

  Unable to configure 1-to-1 VLAN mapping if c-vlan = s-vlan.

  Symptom:

  1-to-1 VLAN mappings are rejected with the following error message:

  ```
  Vlan Translation: invalid parameter
  ```

Condition:

This issue occurs when the value of c-vlan is the same as that of s-vlan. Only the first mapping is accepted, thereafter all 1-to-1 mappings (where the values of c-vlan is the same as that of s-vlan) are rejected with the error "Vlan Translation: invalid parameter".

Workaround:

There is no workaround.

- **CSCud56474**

  Basic Description

  When the IOS image is changed on the Cisco ME-3400E switch, the system does not boot up normally.

  Symptom:

  When the IOS image is changed on the Cisco ME-3400E switch, the system does not boot up normally. The following error message is displayed:

  ```
  POST: Thermal, Fan Tests : Begin" message.
  ```

  Conditions:

  This issue occurs when the IOS image is changed from Cisco IOS Release 12.2(58)SE2 or Cisco IOS Release 12.2(58)EX to Cisco IOS Release 12.2(55)SE6.

  This issue does not occur when the change is from the Cisco IOS Release 12.2(55)SE6 to Cisco IOS Release 12.2(58)SE2.

  Workaround:

  Power off/on to reload the system.

- **CSCud96794**

  Basic Description

  Connectivity Fault Management (CFM) duplicates the MEP in flex link, and Synthetic Loss Measurement (SLM) is not completed when the active link goes down.

  Symptom:

  Connectivity Fault Management (CFM) displays two Maintenance End Points (MEP) with the same remote ID (rmep) although it must display only the active rmep link.

  Also, when the Y.1731 performance monitoring SLM is active in the flex link, and the active port goes down, the standby port takes the active role. However, the standby port does not learn the remote MEPs during this time.

  Conditions:

  This issue occurs when the Up MEP is configured and Up link is a flex link.

  Workaround:

  There is no workaround.

- **CSCue45732**

  Basic Description

  REP ALT port does not block the destination multicast-MAC address—0180.c200.0010.

  Symptom:

Resilient Ethernet Protocol (REP) has Alternate (ALT) as one of the port states. When the REP ALT port receives the multicast MAC address with destination 0180.c200.0010, the port does not block the multicast- MAC address.

Conditions:

This issue occurs in Cisco IOS Release 12.(55)SE3, Cisco IOS Release 12.2(58)SE and Cisco IOS Release 12.2(58)EX.

Workaround:

There is no workaround.

- **CSCue58833**

  Basic Description

  Portchannel interface is not coming up with PPPoEIA in the Cisco ME3400/E-12CS.

  Symptom:

  Port channel and member interfaces are not displayed when PPPoE interface agent is enabled on the Cisco ME3400/E-12CS device.

  Conditions:

  This issue occurs when PPPoE interface agent is enabled while creating an etherchannel interface on the Cisco ME3400-12CS and Cisco ME3400E-12CS devices.

  Workaround:

  There is no workaround.

- **CSCue97775**

  Basic Description

  Port-channel interface flap when the VLAN is added or removed.

  Symptom:

  The port-channel interface flap when adding or removing a VLAN from the trunk on a port-channel interface.

  Condition:

  This issue occurs only when the port-channel interface has interfaces in states other than P or D.

  D – down

  P – bundled in port-channel (member ports are bundled in channel)

  Workaround:

  Shut down the non-P members and make the VLAN changes.

- **CSCug18930**

  Basic Description

  ARP broadcast forwarded on backup interface cause high CPU utilization.

  Symptom:

  High CPU utilization due to interrupts is observed when Dynamic ARP Inspection (DAI) is enabled on any VLAN.

Condition:

This issue is observed on the Cisco ME-3400EG-12CS-M running Cisco IOS Release 12.2(50)SE3. This issue occurs when the DAI is enabled on any VLAN through the **ip arp inspection vlan** command on the active switch.

Workaround:

There is no workaround.

- **CSCug21249**

  Basic Description

  STP BPDUs are not dropped when the non-default native VLAN is shut.

  Symptom:

  The STP/MSTP convergence happens even when the non-default native VLAN is shut or suspended.

  Condition:

  This issue occurs when STP/MSTP is configured on the switch and the switch uses a non-default native VLAN for BPDU convergence.

  This issue is seen only on non-ES ports on the Cisco ME3400 or Cisco ME3750 devices.

  Workaround:

  There is no workaround.

- **CSCug81531**

  Basic Description

  Tracebacks seen while upgrading from 12.2(58)EZ to 12.2(60)EZ.

  Symptom:

  Traceback messages are seen when upgrading from 12.2(58)EZ to 12.2(60)EZ release after reload.

  Condition:

  This issue occurs when the upgrade is from 12.2(58)EZ to 12.2(60)EZ.

  Workaround:

  Reload the new 12.2(60)EZ image.

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.

Note For information about ME 3400 support for ingress QoS classification on QinQ-based ports, see the *Configuring ME 3400E QoS Classification for QinQ-Based Service, Release 12.2(53)SE* document under the ME 3400E Configuration Guides link.

Update to the ME 3400 Hardware Installation Guide

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).

Follow these standard for 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

Updates to the ME 3400E Regulatory Compliance and Safety Information Guide and the Getting Started Guide

These warnings were incorrectly documented in the guides. These are the correct warnings:

All Switches

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
10 A Statement 1005

Cisco ME 3400EG-2CS-A

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:**
140°F (60°C) Statement 1047

Cisco ME 3400E-24TS-M and Cisco ME 3400EG-12CS-M

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:**
149°F (65°C) Statement 1047

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 complete information about the switch and are available from this Cisco.com site:

- Cisco ME 3400E switch:
  http://www.cisco.com/en/US/products/ps9637/tsd_products_support_series_home.html
- Cisco ME 3400 switch:
  http://www.cisco.com/en/US/products/ps6580/tsd_products_support_series_home.html

These are combined documents for the switches:

- *Cisco ME 3400E, ME 3400, and ME 2400 Ethernet Access Switches System Message Guide*

These documents are available for the Cisco ME 3400E switch:

- *Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switches*
- *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400E Ethernet Access Switch Command Reference*
- *Cisco ME 3400E Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400E Ethernet Access Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco ME 3400E Ethernet Access Switch*

These documents are available for the Cisco ME 3400 switch:

- *Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switches*
- *Cisco ME 3400 Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400 Ethernet Access Switch Command Reference*
- *Cisco ME 3400 and ME 2400 Ethernet Access Switch System Message Guide*
- *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco ME 3400 and ME 2400 Ethernet Access Switches*
- *Configuration Notes for the Cisco ME 3400G-12CS Ethernet Access Switch*

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

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.