# Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switches, Cisco IOS Release 12.2(50)SE and Later

**Revised October 5, 2010**

Cisco IOS Release 12.2(50)SE and later runs on the Cisco ME 3400E and ME 3400Series Ethernet Access switches.

These release notes include important information about Cisco IOS Release 12.2(50)SE3 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 3.
- 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 4.

For the complete list of Cisco ME 3400E and ME 3400 switch documentation, see the "Related Documentation" section on page 30.

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

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

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

## Contents

This information is in the release notes:




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

# Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(50)SE.

***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 |
| SFP modules<br>ME 3400 | 1000BASE-T, -BX, -SX, -LX/LH, -ZX<br>100BASE-BX, FX, -LX<br>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<br>1000BASE-LX/LH MMF and SMF<br>1000BASE-SX MMF<br>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<br>Additional DWDM SFPs qualification | Cisco IOS Release 12.2(50)SE |

*Table 1 Supported Hardware (continued)*

| Device | Description | Supported by Minimum Cisco IOS Release |
|---|---|---|
| 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<br>ME 3400E | 1000BASE-BX10, -SX, -LX/LH, -ZX<br>100BASE -BX10, -EX, -FX (GLC-FE-100FX only), -LX10, -ZX<br>1000BASE-T and 10/100/100BASE-T—Category 5,6 (SFP-only ports; not supported on dual-purpose ports)<br>Coarse wavelength-division multiplexing (CWDM)<br>Dense wavelength-division multiplexing (DWDM)<br>Digital optical monitoring (DOM) support for SFP-GE-S, SFP-GE-L, 1000BASE-BX10, 1000BASE-ZX, CWDM and DWDM SFPs<br>**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 |
| 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

These are the procedures for downloading software. 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. 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** The ME 3400 metro base image is not supported on the Cisco ME 3400E switch.

***Table 2 Cisco IOS Software Image Files***

| Filename | Description |
|---|---|
| me340x-metrobase-tar.122-50.SE5.tar | Cisco ME 3400 metro base image.<br>This image has basic Metro Ethernet features. |
| me340x-metrobasek9-tar.122-50.SE5.tar | Cisco ME 3400 metro base cryptographic image.<br>This image has the Kerberos, Secure Shell (SSH), and basic Metro Ethernet features. |
| me340x-metroaccess-tar.122-50.SE5.tar | Cisco ME 3400E and ME 3400 metro access image.<br>This image has Layer 2 + Metro Ethernet features. |
| me340x-metroaccessk9-tar.122-50.SE5.tar | Cisco ME 3400E and ME 3400 metro access cryptographic image.<br>This image has the Kerberos, SSH, and Layer 2 + Metro Ethernet features. |
| me340x-metroipaccess-tar.122-50.SE5.tar | Cisco ME 3400E and ME 3400 metro IP access image.<br>This image has Layer 2+ and full Layer 3 routing Metro Ethernet features. |
| me340x-metroipaccess9-tar.122-50.SE5.tar | Cisco ME 3400E and ME 3400 metro IP access cryptographic image.<br>This image has the 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/partner/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html#wp1018426

# Upgrading a Switch

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. See the "New Software Features" section on page 7 for a definition of NNIs and UNIs.

To download software, follow these steps:

**Step 1** Use Table 2 on page 4 to identify the file that you want to download.

**Step 2** Download the software image file. If you have a SmartNet support contract, log in to cisco.com and go to this URL, and log in to download the appropriate files:

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

Click on "*Launch the IOS Upgrade Planner*" and search for the ME3400 platform to select the appropriate files:

- Select the software release and image you want to download.
- You might need to obtain authorization and to download the cryptographic software files

**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 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite

tftp://198.30.20.19/me340x-metroipaccess-tar.122.50.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

## Recovering from a Software Failure

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 using these methods:

- The CLI-based setup program, as described in the switch hardware installation guide.
- 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 Features

These sections describe the new supported hardware and the new software features provided in this release:


- New Hardware Features, page 6
- New Software Features, page 7


## New Hardware Features

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

## New Software Features

- IPv6 routing support (requires metro IP access image):
  - DHCP for IPv6 relay, client, server address assignment and prefix delegation
  - IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces using static routing, RIP, OSPF, or EIGRP
  - IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router

**Note** Although documented in the software configuration guide, HTTP(S) over IPv6 is not supported in this release.

- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic (requires metro IP access image).
- Bidirectional Forwarding Detection (BFD) Protocol to quickly detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols.
- REP configuration on edge ports connected to ports that do not support REP.
- Support for Embedded Event Manager Version 2.4.
- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- CPU utilization threshold trap monitors CPU utilization.
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Support for the CISCO-ENTITY-SENSOR MIB and the CISCO-PORT-QOS-MI**B**
- IP source guard in the metro base image (ME 3400) to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection in the metro base image (ME 3400) to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN

# Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release (after the first release) required to support the major 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 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 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)<br>12.2(50)SE (ME 3400E) |
| REP counter and timer enhancements | 12.2(46)SE (ME 3400)<br>12.2(50)SE (ME 3400E) |
| HSRPv2 (metro IP access image only) | 12.2(46)SE (ME 3400)<br>12.2(50)SE (ME 3400E) |
| DHCP server port-based address allocation | 12.2(46)SE (ME 3400)<br>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)<br>**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 |

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

| Feature | Minimum Cisco IOS Release Required |
|---|---|
| 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 |
| 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 switchover (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 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

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

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

## 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)

# 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)

## 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)

## 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.

## 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)
- Although visible in the command-line help, the **conform-action color** *class-map* police configuration command is not supported. Entering the command has no affect.

  There is no workaround. (CSCsk00594)
- 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 the recommended limit of 13,000, the switch can fail.

  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)

# Open Caveats

- CSCsk58435

  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.

- CSCsv24288 (ME 3400E)

  If you create a QoS configuration that uses more than the platform limit of 256 unique policer profiles (unique combinations of rates and actions), the policy map that caused the hardware resource exhaustion is rejected. Further attempts to attach new policies are also rejected. This occurs even if you modify the policy that caused the resource exhaustion to use less resources.

  The workaround is to modify the existing policy maps to use less than 256 unique policer profiles and to reload the switch to free up the hardware resources.

- CSCsw77908 (ME 3400E)

  When you configure an aggregate policer in a per-port per-VLAN service policy, the output of the **show policy-map interface** privileged EXEC command displays zeroes for the policer rate counters. This occurs only when the policer is an aggregate policer and the service policy is hierarchical.

  There is no workaround.

- CSCsw91409 (ME 3400E)

  On an ME 3400E-2CS or ME 3400E-12CS switch, a port-shaper configured for 500 K bits per second (Kb/s) on a 100 Mb/s link shapes at approximately 90 Kb/s. Port shapers at 1 Mb/s and higher function correctly. This occurs only on the 2CS and 12CS platforms when the link speed is 100 Mb/s and the configured shape rate is 500Kb/s.

  The workaround is to configure the shaper for 1Mb/s or higher or to change the link speed to 10Mb/s.

- CSCsw68528

  When you enter the **show mvr interface** *interface-id* **members** privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as *ACTIVE*.

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

- CSCsw69015

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

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

- CSCsx18055 (ME 3400)

  A `Hardware resources are not available` message appears under these conditions:

  - VLANs are created in a group and assigned to the UNI-VLAN community.
  - Those VLANs are deleted.
  - You recreate those VLANs again and reassign them to the UNI-VLAN community again.

  There is no workaround.

- CSCsx06575

  If an RSPAN interface is configured as an MVR source port (configured by entering the **mvr type source** interface configuration command), RSPAN receives captured data through the RSPAN VLAN, but does not send the packets to the RSPAN destination interface. The same limitation also applies to monitoring IGMP snooping groups or multicast routing groups.

  The workaround is to disable MVR on all RSPAN uplink interfaces by entering the **no mvr type** interface configuration command and to not monitor traffic in an MVR group, an IGMP snooping group, or a multicast routing group.

- CSCta39338

  Entering the **udld enable** global configuration command is supposed to enable UniDirectional Link Detection (UDLD) only on fiber ports. You enter the **udld port** interface configuration command to enable UDLD on other port types. However, when you enter the **udld enable** global configuration command, UDLD is enabled by default on dual-media ports, even if a copper link is connected to an RJ-45 socket.

  The workaround is to manually disable UDLD on the port by entering the **no udld port** interface configuration command.

- CSCta57846

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

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

- CSCti79385

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

  There is no workaround.

# Resolved Caveats

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

- CSCte14603

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

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

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

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

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

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

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

- CSCsh59019

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

  There is no workaround.

- CSCsk85192

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

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

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

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

- CSCsx31345

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

  There is no workaround.

- CSCsx97605

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

  There is no workaround.

- CSCsy15256

  If a switch is directly connected to another switch and both are running Cisco IOS IP Service Level Agreements (SLAs) to monitor jitter, a message about high jitter appears and then the problem is resolved automatically when the event does not occur:

  ```
  036814: Feb 11 23:30:04: IP SLAs (10) jitter operation: seq=12, jitterIn=44
  036820: Feb 11 23:30:05: IP SLAs (10) jitter operation: seq=13, jitterIn=-44
  ```

  There is no workaround.

- CSCsy83366

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

  There is no workaround.

- CSCsy90265

  If you repeatedly enter the **show tech-support** privileged EXEC command, the switch might leak memory and, in some cases, shut down.

  The workaround is to reload the switch to clear the memory after repeated use of the **show tech-support** command.

- CSCsz66428

  When flow control is enabled on a port-channel interface and you enter the flowcontrol receive on interface configuration command, the bundle is not enabled after the switch restarts. The command appears in the port-channel interface running configuration but does not appear in the switch running configuration. A message such as this appears:

  ```
  %EC-5-CANNOT_BUNDLE2: Gi0/27 is not compatible with Po1 and will be suspended (flow
  control receive of Gi0/27 is on, Po1 is off)
  %EC-5-CANNOT_BUNDLE2: Gi0/28 is not compatible with Po1 and will be suspended (flow
  control receive of Gi0/28 is on, Po1 is off)
  ```

  Use one of these workarounds:

  - To manually configure the port-channel interface, enter the flowcontrol receive on interface configuration command.
  - To add the flow-control configuration to the interface after the switch restarts, use an EEM script similar to this:

    ```
    event manager applet Add_flowcontrol_on_restart
    event syslog pattern SYS-5-RESTART
    action 1 cli command "en"
    action 2 cli command "conf t"
    action 3 cli command "inter port 1"
    action 4 cli command "flowcontrol receive on"
    ```

    For *action 3*, specify the port-channel interface.

- CSCsz72234

  In a VPN routing/forwarding (VRF) instance, a port channel is configured, and the default route is in the global routing table. If a link shuts down while the other links remain up, the port channel might not forward traffic.

Use one of these workarounds:

- Enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command.
- In the VRF instance, configure the links in the port channel as Layer 2 access links, and configure a switch virtual interface (SVI).

- CSCta09189

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

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

  Use one of these workarounds:

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

- CSCta57846

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

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

- CSCta78502

  When you have configured a login banner by entering the **banner login** *c message c* global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.

  There is no workaround.

- CSCtb10158

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

  There is no workaround.

- CSCtb77378

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

  The workaround is to remove the custom banner.

- CSCtb78951

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

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

- CSCtb91572

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

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

- CSCtc39809

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

  There is no workaround.

- CSCtc43231

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

  There is no workaround.

- CSCtc57809

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

  - The physical interface is in a *no shut* state.
  - The MAC address is first dynamically learned and then changed to static.

  There is no workaround.

- CSCtc70571

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

- CSCtc90039

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

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

- CSCtd17296

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

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

- CSCtd30053

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

  There is no workaround.

- CSCtd31242

  An IP phone loses network connectivity under these conditions:

  - The IP phone is authenticated by MAB (in Open1x mode) on a supplicant switch.
  - The supplicant switch is connected to an authenticator switch through the NEAT protocol.

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

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

- CSCtd34310

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

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

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

  There is no workaround.

- CSCtd50287

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

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

- CSCtd72456

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

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

- CSCtd72626

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

  There is no workaround.

- CSCtd73256

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

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

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

  When the switch fails, it sends this error message:

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

  There is no workaround.

- CSCte67201

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

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

- CSCte81321

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

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

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

- CSCsl72774

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

  **cef table consistency-check ipv4**

  **cef table consistency-check ipv6**

- CSCso57496

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

- CSCso90107 (ME 3400)

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

- CSCsq24002

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

- CSCsq51052 (ME 3400)

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

- CSCsw45277

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

- CSCsx49718

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

  - The port is in single-host mode.
  - The port is configured with the **authentication event no-response action authorize vlan** *vlan-number* command.
  - An EAPOL start packet is sent to the port.

- CSCsx70889

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsx94339

  A switch no longer fails and reloads when a specific queue is removed from a class:

```
class-map match-any CMAP-BC-ALL-COS
 match cos  2
 match cos  1

policy-map PMAP-ingress-g0/1
  class CMAP-BC-ALL-COS
    no queue-limit cos  1 200
```

- CSCsy07555

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsy15227

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

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

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

- CSCsy48370

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

- CSCsy53381

  Ping packets are no longer accepted on user network interfaces (UNIs) or enhanced network interfaces.

- CSCsy72669

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

- CSCsy91579

  A switch no longer randomly resets due to memory corruption.

- CSCsz08054

  QoS scheduling policies assigned to ports that are members of a port-channel now work correctly. In previous releases, only the default “equal and fair” scheduling policy was applied to port-channel members, even though a configured QoS scheduling policy was assigned.

- CSCsz12381

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

- CSCsz13490

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

- CSCsz14369

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

- CSCsz43495 (ME3400E)

  When a IEEE 802.1Q tunnel is set in a Resilient Ethernet Protocol (REP) ring, Address Resolution Protocol (ARP) broadcast loops no longer occur in the REP topology, and SW_MATM-4-MACFLAP_NOTIF messages no longer appear.

- CSCsz79652

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

- CSCsz81762

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

- CSCta36155

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

- CSCta56469

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

- CSCta67777

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

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

- CSCsy24510

  The switch now accepts an encrypted secret password.

- CSCsr92741

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

- CSCsb46724

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

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

- CSCsi01526

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

- CSCsk53850

  If you enter the **no ip vrf** *vrf-name* global configuration command to delete a VPN routing/forwarding instance on the switch when routing is not enabled on the switch, the VRF instance is no longer held in the delete queue and using one of the system's maximum allowable VRFs.

- CSCsq26873

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

- CSCsq67398

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

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

- CSCsq89564

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

- CSCsr22987

  A switch no longer intermittently fails and displays an error message when the **uni-vlan community** configuration is in the switch running configuration.

- CSCsr50766

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

- CSCsr64007

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

- CSCsr65689

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

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

- CSCsu88168

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

- CSCsv04836

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

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

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsv64023

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

- CSCsv65793

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

- CSCsv89005

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

- CSCsw30249

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

- CSCsw65548

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

- CSCsx12513 (ME-3400G-12C only)

  Traffic subject to quality of service (QOS) configuration is now handled as expected.

# Documentation Updates



## Update to the Software Configuration Guide

Although documented in the software configuration guide, HTTP(S) over IPv6 is not supported in this release.

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

## Update to the ME 3400 Hardware Installation Guide

This is an installation update to the *Cisco ME3400 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).

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

# Updates to the System Message Guide

These messages were added but are not yet in the system message guide:

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

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

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

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

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

**Recommended Action** No action is required.

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

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

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

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

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

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

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

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

– To delete one of the VLANs with an STP instance, enter the **no vlan** *vlan-id* global configuration command.

– To disable spanning tree on a per-VLAN basis. enter the **no spanning-tree** *vlan-id* global configuration command.

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

These messages were deleted:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 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

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

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 Ethernet Access Switch*
- *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:

- *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

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.