Release Notes for the Cisco ME 3800X and ME 3600X Switch, Cisco IOS Release 12.2(52)EY and Later Releases

January 22, 2013

These release notes include important information about the following Cisco IOS releases that run on the Cisco ME 3800X and ME 3600X switches:

- Cisco IOS Release 12.2(52)EY
- Cisco IOS Release 12.2(52)EY1
- Cisco IOS Release 12.2(52)EY1b
- Cisco IOS Release 12.2(52)EY1c
- Cisco IOS Release 12.2(52)EY2
- Cisco IOS Release 12.2(52)EY2a
- Cisco IOS Release 12.2(52)EY3
- Cisco IOS Release 12.2(52)EY3a
- Cisco IOS Release 12.2(52)EY4

These release notes also include the limitations, restrictions, and caveats that apply to these releases.

You can verify that these release notes apply to your switch as follows:

- 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 4.
- If you are upgrading to a new release or a 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 3800X and ME 3600X switch documentation, see the "Related Documentation" section on page 33.

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=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

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

Contents

Hardware Supported

Table 1 Supported Hardware

Device	Description
Cisco ME-3800X-24FS-M	24 Gigabit Ethernet SFP downlink ports and 2 SFP+ (10 Gigabit) uplink ports; supports removable, hot-swappable AC- and DC-input power supplies and fan modules.
Cisco ME-3600X-24FS-M	24 Gigabit Ethernet SFP downlink ports and 2 SFP+ (10 Gigabit) uplink ports; supports removable, hot-swappable AC- and DC-input power supplies. and fan modules
Cisco ME-3600X-24TS-M	24 10/100/1000BASE-T copper downlink ports and 2 SFP+ (10 Gigabit) uplink ports; supports removable, hot-swappable AC- and DC-input power supplies and fan modules.
SFP+ modules	SFP-10GE-SR, SFP-10GE-LR, SFP-10GE-LRM,SFP-H10GB-CUxM, SFP-10G-ER
SFP modules	GLC-FE-100FX, GLC-FE-100EX, GLC-FE-100ZX, GLC-FE-100LX, GLC-FE-100BX-U, GLC-FE-100BX-D, GLC-LHSM, GLC-SX-MM, GLC-ZX-SM, GLC-T, CWDM-SFP-1470, CWDM-SFP-1490, CWDM-SFP-1510, CWDM-SFP- 1530, CWDM-SFP-1550, CWDM-SFP-1570, CWDM-SFP-1590, CWDM-SFP-1610, GLC-BX-U, GLC-BX-D, SFPGE- L,SFP-GE-S, SFP-GE-T, DWDM-SFP-xx
Cables	SFP interconnect cable (50 cm) 1-meter, 3-meter, and 5-meter copper SFP+ cables

Software Licenses and Features

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image, available in crypto and noncrypto versions. If you do not have a service support contract, such as a SMARTnet contract, download the image from Cisco.com.

The ME 3600X supports these licenses:

- Metro IP access is the universal image.
- Advanced Metro IP access license.
- 10 Gigabit Ethernet upgrade license—enables 10 Gigabit Ethernet on the SFP+ uplink ports.

For differences in feature support for each license, see Table 2 and Table 3 on page 3.

The ME 3800X supports these licenses plus a scaled license that can be installed with any of these licenses to increase the supported values for that license, for example, more MAC addresses, VLANs, IPv4 routes, and so on.

- Metro Ethernet services is the universal image.
- Metro IP service license.
- Metro Aggregation services license.
- Scaled license for any of the above licenses

For differences in feature support for each license, see Table 4 and Table 5 on page 4.

To install a software image, see the "Upgrading the Switch Software" section on page 4 and the "Working with the Cisco IOS File System, Configuration Files, and Software Images" chapter in the software configuration guide.

To install a software license, see the "Cisco IOS Software Activation Tasks and Commands" chapter in the Cisco IOS Software Activation Configuration Guide:

http://www.cisco.com/en/US/docs/ios/csa/configuration/guide/12.4T/csa_book.html

Table 2 ME 3600X Supported Features per License

Metro IP Access (Universal Image)	Advanced Metro IP Access license
• Basic Layer 2 features (including 802.1Q) • Ethernet Virtual Circuits (EVCs) • IPv4 routing—RIP, OSFP, EIGRP, IS-IS, and BGP • Bidirectional Forwarding Detection (BFD) • Multicast routing —PIM, DM, SSM, and SSM mapping • Ethernet Operations, Administration, and Maintenance (OAM)—802.1ag, 802.3ah, and E-LMI • Multiple Spanning Tree Protocol (MSTP), Resilient Ethernet Protocol (REP), and Flex Links • Synchronous Ethernet • Multi VRF-CE (VRF-Lite) with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)	• All features in the Metro IP Access image • Multiprotocol label switching (MPLS) • MPLS traffic engineering and Fast Reroute • MPLS OAM • MPLS VPN • Ethernet over MPLS (EoMPLS) • Pseudowire redundancy

Table 3 ME 3600X License Scaling

Supported feature	Metro IP Access	Advanced Metro IP Access
MAC addresses	8 K	16 K
IPv4 routes	20 K	20 K
IPv4 multicast groups and routes	1 K	1 K
Layer 2 multicast entries	1 K	1 K
Bridge domains	4 K	4 K
ACL entries	2 K	2 K

Table 4 ME 3800X Supported Features per License

Metro Ethernet Services (Universal Image)	Metro IP Services license	Metro Aggregation Services license
• Basic Layer 2 features (including 802.1d and 802.1Q) • EVCs • Ethernet OAM—802.1ag, 802.3ah, and E-LMI • MST, REP, Flex Links • Synchronous Ethernet	• All features in the Metro Ethernet Services image • IPv4 routing—RIP, OSFP, EIGRP, IS-IS, and BGP • BFD • Multicast routing—PIM, DM, SSM, and SSM mapping • Multi VRF-CE with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)	• All features in the Metro IP Services license • MPLS • MPLS traffic engineering and Fast Reroute • MPLS OAM • MPLS VPN • EoMPLS • Pseudowire redundancy

Table 5 ME 3800X License Scaling

Supported feature	Metro Services	Scaled Metro Services	Metro IP Services	Scaled Metro IP Services	Metro Aggregation Services	Scaled Metro Aggregation Services
MAC table addresses	64 K	128 K	32 K	64 K	128 K	256 K
IPv4 routes	1 K	1 K	42 K	80 K	24 K	32 K
IPv4 multicast groups and routes	0	0	2 K	4 K	2 K	4 K
Layer 2 multicast entries	2 K	4 K	2 K	2 K	2 K	4 K
Bridge domains	4 K	4 K	2 K	2 K	4 K	8 K
ACL entries	4 K	8 K	4 K	8 K	4 K	16 K

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:).

Note The flash memory can store a maximum of two IOS images or tar files. If you try to copy or archive upgrade beyond the flash memory capacity, the action aborts.

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 software installation 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 6 Cisco IOS Software Image Files

Filename	Description
me380x-universal-tar.122-52.EY.tar	Cisco ME 3800X universal images.
me380x-universal-tar.122-52.EY1.tar	
me380x-universal-tar.122-52.EY1b.tar	
me380x-universal-tar.122-52.EY1c.tar	
me380x-universal-tar.122-52.EY2.tar	
me380x-universal-tar.122-52.EY2a.tar	
me380x-universal-tar.122-52.EY3.tar	
me380x-universal-tar.122-52.EY3a.tar	
me380x-universal-tar.122-52.EY4.tar	
me380x-universalk9-tar.122-52.EY.tar	Cisco ME 3800X universal cryptographic images. These images have the Metro Ethernet features plus Kerberos and SSH.
me380x-universalk9-tar.122-52.EY1.tar	
me380x-universalk9-tar.122-52.EY1b.tar	
me380x-universalk9-tar.122-52.EY1c.tar	
me380x-universalk9-tar.122-52.EY2.tar	
me380x-universalk9-tar.122-52.EY2a.tar	
me380x-universalk9-tar.122-52.EY3.tar	
me380x-universalk9-tar.122-52.EY3a.tar	
me380x-universalk9-tar.122-52.EY4.tar	

Table 6 Cisco IOS Software Image Files (continued)

Filename	Description
me360x-universal-tar.122-52.EY.tar me360x-universal-tar.122-52.EY1.tar me360x-universal-tar.122-52.EY1b.tar me360x-universal-tar.122-52.EY1c.tar me360x-universal-tar.122-52.EY2.tar me360x-universal-tar.122-52.EY2a.tar me360x-universal-tar.122-52.EY3.tar me360x-universal-tar.122-52.EY3a.tar me360x-universal-tar.122-52.EY4.tar	Cisco ME 3600X universal images.
me360x-universalk9-tar.122-52.EY.tar me360x-universalk9-tar.122-52.EY1.tar me360x-universalk9-tar.122-52.EY1b.tar me360x-universalk9-tar.122-52.EY1c.tar me360x-universalk9-tar.122-52.EY2.tar me360x-universalk9-tar.122-52.EY2a.tar me360x-universalk9-tar.122-52.EY3.tar me360x-universalk9-tar.122-52.EY3a.tar me360x-universalk9-tar.122-52.EY4.tar	Cisco ME 3600X universal cryptographic images. These images have the Metro IP access features plus Kerberos and SSH.

Installing Software Images and Licenses

The switch is shipped with the latest software image installed. Follow the instructions in this section if you need to reinstall or upgrade the software image.

Before installing 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 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/docs/ios/fundamentals/command/reference/cf_t1.html

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.

To download software, follow these steps:

Step 1 Use Table 6 on page 5 to identify the file that you want to download.

Step 2 Locate 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=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

b. For ME 3800X, navigate to **Switches > Service Provider Switches - Ethernet Aggregation**.

For ME 3600X, navigate to **Switches > Service Provider Switches - Ethernet Access**.

c. Navigate to your switch model.

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

Note When you select a crypto image, you must also accept the terms and conditions of using crypto images.

Step 3 Download the image to a TFTP server and make sure that the 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
```

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 by entering this privileged EXEC command:

```
Switch# archive download-sw tftp:[[//location]/directory]/image-name.tar
```

- 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.
- 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.

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.

Note There can be only two image directories in flash memory.

The installation process extracts the tar file with all the files and the IOS image, and sets the BOOT directory to the created directory in flash memory. The process takes approximately 5 to 10 minutes, and at some stages might appear to have stopped.

Step 7 The switch is configured to boot automatically, but you can ether the **show boot** privileged EXEC command to verify the boot path list and see if a manual boot is necessary.

```
Switch# show boot
BOOT path-list      :
flash:/me380x-universal-mz.122-52.EY/me380x-universal-mz.122-52.EY.bin
Config file         :    flash:/config.text
Private Config file : flash:/private-config.text
Manual Boot         : no
HELPER path-list    :
```

Step 8 Save the configuration and reload the switch.

```
Switch# reload
```

After the installation, the switch is running the universal image. Follow these steps to install a purchased license with increased capabilities. To purchase a license, contact Cisco.

Step 1 Copy the license file to flash or TFTP.

Step 2 Enter the command to install the license:

```
Switch# license install flash:LICENSE_FILENAME
or
Switch# license install tftp://location/LICENSE_FILENAME
```

Step 3 Enter these commands to boot from the new license:

```
Switch# configure terminal
Switch(config)# license boot level license_name
```

Step 4 If you have a a scaled license, install the scaled license

```
Switch# license install flash:SCALED_LICENSE_FILENAME
or
Switch# license install tftp://location/SCALED_LICENSE_FILENAME
```

Note To revert to a non-scaled license, enter the **license clear** *scaled_license_name* privileged EXEC command.

Step 5 Reload the switch for new license to take effect.

```
Switch# reload
```

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 Software Features

This release is the second software release for the Cisco ME 3800X and ME 3600X switch. For a detailed list of key features for this software release, refer to the "Overview" chapter of the software configuration guide for this release.

Important Notes

- Approximately five minutes after the box boots up the IOS configuration, the on-board failure logging (OBFL) processes initializes, which uses CPU resources. This causes the switch to be less responsive for other functions for a short time.
- If you try to configure more MPLS labels than are supported by the license installed on the switch, you might see a message similar to this:

  ```
  *Mar  1 00:08:02.332: %SW_MGR-3-CM_ERROR: Connection Manager
  Error - provision segment failed [ADJ:Vlan:2101760] - hardware platform error.
  ```

  This does not affect functionality, but is a reminder that the number of MPLS labels is exceeding the limit.
- 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:
  - 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.
- In ME3800X platform, Cisco IOS Release 12.2(52)EY, the forward keyword is not supported for the l2protocol command. Therefore, it is impossible to forward Layer 2 control packets from a ME3800X switch to a Cisco 7600 router and vice versa. The tunnel option in ME3800X overwrites the PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0), while the forward option in Cisco 7600 simply forwards the PDU without any change or local processing; thus, the two platforms cannot cooperate.
- Switch Port Analyzer (SPAN) is not supported.

Resolved and Open Caveats

The following sections provide information on resolved and open caveats:

- Resolved Caveats for Cisco IOS Release 12.2(52)EY4, page 10
- Resolved Caveats for Cisco IOS Release 12.2(52)EY3a, page 16
- Resolved Caveats for Cisco IOS Release 12.2 (52) EY3, page 16
- Open Caveats for Cisco IOS Release 12.2 (52) EY2a, page 19
- Resolved Caveats for Cisco IOS Release 12.2 (52) EY2a, page 19
- Open Caveats for Cisco IOS Release 12.2 (52) EY2, page 20

Resolved Caveats for Cisco IOS Release 12.2(52)EY4

The following are resolved in Cisco IOS Release 12.2(52)EY4:

- CSCtt28591

  Interface does not come up with duplex full and connected with crossover cable.

  Interface does not come up when duplex is set to full and connected with crossover cable.

  Workaround: shutdown/no shutdown

- CSCtt30722

  New number cannot be assigned to loopback IF on ME3600.

  New number cannot be assigned to loopback Interface on ME3600 where 64 numbers have been used and assigned to loopback interfaces.

  Workaround: None.

- CSCtn77721

  Router crashes on defaulting interface with BFD on HSRP.

- CSCtt40711

  CLI for getting PVR/SVR values for PPC.

  Sometimes **show version** command does not show the correct revision for PPC. This issue is intermittent.

  Workaround: None.

- CSCtt94445

  Cannot re-configure class-default under policy-map.

  no class class-default

  Workaround:

  1. Delete and re-configure the policy-map.
  2. Delete and re-configure the **police cir** command.

- CSCtr61781

  I/P traffic statistics getting classified under I/P policy-map applied on O/P.

  Statistics gets incremented for the incorrect class in a different policy-map.

  This issue occurs when there is an input policy and an output policy defined on the incoming and outgoing interfaces respectively. If you remove the egress policy and attach an input policy to the egress interface, then traffic increments on the input policy of input interface when the traffic is reversed.

  Workaround: None.

- CSCts79107

  Switch blocks DHCP packets with broadcast flag.

  DHCP packets with broadcast flag are blocked by the switch.

  This occurs on the ME-3600X-24FS-M switch, where the DHCP relay is configured using the **switchport block multicast** command.

  Workaround: Use the **no switchport block multicast** command.

- CSCtt03126

  ME 3600X not passing Multicast packets to 224.0.0.x through EVC configuration

  Unicast traffic and multicast traffic except 224.0.0.x pass through without any issues. This has been observed on tengigabit interface on ME3600 under the following conditions:

  - Bridge Domain is greater than 4094 or
  - Spanning tree mode is not MST or
  - Packets coming into the ME 3600 are untagged.

  Workaround:

  - Make sure that the packets coming into the ME3600X are tagged with vlan id. If it is an L3 port, then create a sub-interface and configure encapsulation dot1q vlan.
  - Configure Spanning Tree mode as MST.
  - Bridge Domain should be less than 4094.

- CSCtt98501

  ME3600: backup PW (svi connect) flap crashes the box.

  ME3600/ME3800 crashes with mac learning happening on SVI pseudowires, and ospf/bgp/ldp flaps or reconverges at the same time. This is predominantly seen when backup pseudowires are configured but can also occur on normal SVI pseudowires.

  Workaround: Disable mac learning on SVI VLANs.

- CSCto13426

  ME3800 SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error.

  The following log message and tracebacks may be seen:

  ```
  SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment
  class.
  -Traceback= 7088F4z 1801754z 18015D8z 27DCD54z 2BFDADCz 2C05C04z 413500z 28B9508z
  28B958Cz 3B1F30z 3B22B4z 3B26A8z 3B2728z 3B2788z 3B4B88z 3B4958z
  ```

  This may be seen on an ME3800 device that is using pseudowires and EVCs in the configuration.

  Workaround: Reload the device. However, in come cases the device may reload however OSPF neighbors may not form a full OSPF neighbor relationship after this traceback occurs.

- CSCto10254

  ME3600/ME3800 router stuck at t/b -Process= "Collection process" on ospf shut.

- CSCtu02164

  Rep fails periodically on TenGigabit port.

  REP enabled TE port on ME3600/ME3800 goes to failed state without any trigger. TE port on ME3600/ME3800 fails without any condition, just REP enabled.

This issue is seen only when a 1000Base SFP is used with the TenGigabit port. It is not seen with Gigabit interfaces.

Workaround: Shut/No shut is a temporary workaround. The issue occurs again after a day or two.

- CSCto96311

  ME3600/ME3800 crash@oce_to_sw_obj_type on frr cutover.

  When attempting to trigger FRR by shutdown/no shutdown of one of the gigabit links, the switch crashes.

  Workaround: None.

- CSCtr20229

  ME3600/ME3800 switch crashed after prolonged TE interface flapping.

  Workaround: None.

- CSCtr58677

  ME3600/ME3800 switch crashes due to cpu-hog by collection process.

  Workaround: None.

- CSCtu31659

  ME3600 switch crashes with **diagnostic start test all** command.

  ME-3600X series switch running 12.2(52)EY2 and/or 15.1(2)EY IOS release crashes when the **diagnostic start test all** command is entered in the CLI. There are no specific configurations which trigger this error, the switch crashes with empty configuration.

  Workaround: Avoid running the **diagnostic start test all** command on vulnerable code. Code upgrade needed when the fix is available.

- CSCtg48785

  show x25 hunt-group command causes %DATACORRUPTION-1-DATAINCONSISTENCY: copy error

  When issuing the **show x25 hunt-group** command, the following error may appear:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  Workaround: None.

- CSCtt99101

  Management port stops responding due to O/P queue wedge 40/40.

  Issue is seen after 4-5 days when the box is up and traffic is passing via management port.

  Workaround: Reload the box.

- CSCtu64927

  CHUNKBADMAGIC seen for collection process.

  This message is seen at collection process when the core interface is flapped and the core IGP comes up.

  Workaround: None.

- CSCsu29708

  122SRD: **Show dot1q-tunnel** command with 2 act tunnel ports crashes SUP.

  Tracebacks are seen when **show dot1q-tunnel** is executed.

Workaround: None.

- CSCtn55054

  DATA Corruption image with SXI5a throttle image.

  Workaround: None.

- CSCtg57764

  Traceback while setting cdsRelayAgentInfoOptRemoteIdSub to more than 63.

  Setting the cdsRelayAgentInfoOptRemoteIdSub to more than 63 results in traceback on DUT console.

  Workaround: Retrieve the size using **ip dhcp snooping information option format remote-id string** command.

- CSCtu22952

  Traffic stops forwarding with EFP over multiple member link LACP bundle.

  A Cisco ME3800 may stop forwarding traffic. The problem occurs when a Port-channel interface with multiple member link on LACP is configured via EVC. By sending single Source-Destination traffic, it is seen to be moving from one member link to another.

  Workaround:

  - Use etherchannel instead of LACP.
  - Remove EVC.

- CSCtu36333

  ME36xx console not working at speed 300.

  A baud rate less than 1200 is not supported on ME36xx platform. The supported baud rate range is 1200 - 115200, the default baud rate is 9600.

  Workaround: None.

- CSCtr51496

  ME3600/ME3800 QoS: Memory Leaks on DM of the policy-map.

  Workaround: None.

- CSCtw85509

  ME3600 show process xxx are Ambiguous command in show tech.

  On the ME-3600X-24FS-M switch running Cisco IOS Release 15.1(2)EY1, the following command's log is not displayed by the **show tech** command.

  show process memory

  show process cpu

  show process cpu history

  If you enter **show process xxx** command only, the command displays the following output:

  ```
  Switch# show process cpu
  % Ambiguous command: "show process cpu"
  ```

  Workaround: Use the following commands:

  show processes memory

  show processes cpu

  show processes cpu history

- CSCtw74099

  ME3600X crashes with ttl macro and SNMP access.

  Switch will crash if the etsec tx ring is hanged with the below TB decodes:

  ```
  0x21F0DFC:etsec_tx_freeze_check_process(0x21f0d94)+0x68
  0x2B620C8:ppc_process_dispatch(0x2b620a4)+0x24
  0x2B5C830:process_execute(0x2b5c5e8)+0x248
  ```

  Workaround: Shut down the management port.

- CSCtw53043

  QoS: Policer configuration has exceeded hardware limitation.

  The ME-3800X-24FS-M switch running Cisco IOS Release 12.2(52)EY2 displays the following output when a service policy is applied:

  ```
  ECBUDECSCR11(config)# policy-map NNI-GI0/1-IN
  ECBUDECSCR11(config-pmap)# class 152
  ECBUDECSCR11(config-pmap-c)# service-policy VLAN152
  QoS: Policer configuration has exceeded hardware limitation. The max number of ingress
  policers supported for interface range Gig0/1-Gi0/24 is 4096.
  QoS: Configuration failed. Can NOT allocate resources.
  QoS: Policy attachment failed. Configuration exceeds hardware resources for policy
  VLAN152
  ```

  However the limit of 4096 policers have not been configured on the switch.

  Workaround: None.

- CSCsv82825

  copy running-config startup-config gives 0 bytes copied.

  Workaround: None.

- CSCtw79815

  Mem leak at nile_qm_alloc_eqos_vmr_entry during router bootup.

  Memory leaks observed after bootup. The memory leaks are observed at nile_qm_alloc_eqos_vmr_entry.

  Workaround: None.

- CSCtw94853

  Buffer leak on ME3600X due to **no VTP** enabled.

  ME3600X running Cisco IOS Release 12.2(52), with **no VTP** command configured on the interface will have buffer leak due to receiving VTP packets.

  Workaround: Enable VTP on interface.

- CSCtu02455

  ME3600X: Egress QoS service-policy classify 'marked' packet incorrectly.

  Egress QoS service-policy does not classify marked packet correctly when applied to Layer 3 port channel members. The issue is seen only when the port channel is layer 3.

  Workaround:

  - Remove and reapply the service-policy on the member interfaces.

    OR

  - Use a layer-2 port-channel and use SVI for layer 3 peering.

- CSCtt31368

  ME3600 wrong optical alarm Thresholds for CWDM SFPs.

  CWDM sfps on a ME3600 switch, the optical receive alarm levels do not correspond to the data sheet levels for this SFPs.

  Workaround: None.

- CSCtu72323

  Add show logging in **show tech-support** command for ME3600 and ME3800.

  Workaround: None.

- CSCtx42616

  ME3600 switch with optical SFP media can not enable receive flow control.

  Flow-control negotiation setting is ignored when optical SFP is used.

  Workaround: None.

- CSCtx91780

  ME3600/3800 tar image build failure occurs on LDS servers.

  Workaround: None.

- CSCtr28857

  MSDP-peered router joined to a multicast group may crash.

  A Cisco router crashes when the Multicast Source Discovery Protocol (MSDP) multicast routing is enabled.

  This issue is seen when a Cisco router is configured with MSDP multicast routing and the router is explicitly joined to the multicast group.

  Workaround: Disable **ip sap listen**, and do not execute the **ip igmp join-group 224.2.127.254** command.

- CSCtr91106

  Command Authorization Fails for commands delivered over HTTP.

  A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS software are not vulnerable. Cisco has released free software updates that address these vulnerabilities. The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 8.5/7:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-0384 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Resolved Caveats for Cisco IOS Release 12.2(52)EY3a

The following is resolved in Cisco IOS Release 12.2(52)EY3a:

- CSCtt21887

  rfp fail multicast copy Egress Port Queue and it causes packets drop.

  rpf failed packets copy to SVI port which have rpf-fail oif list. It causes output queue exhaustion. The Router has SVI I/F with PIM enable and receives Join. The router receives the rfp fail packets.

  Workaround: None.

Resolved Caveats for Cisco IOS Release 12.2 (52) EY3

The following caveats are resolved in Cisco IOS Release 12.2(52) EY3:

- CSCts08326

  Claim support for both CISCO-PORT-QOS-MIB and CISCO-CLASS-BASED-QOS-MIB.

  When access to CISCO-PORT-QOS-MIB and CISCO-CLASS-BASED-QOS-MIB, some of OID does not reply.

  Workaround: None.

- CSCts91603

  On ME3600/3800 rpf fail packets are double accounted on qos policies of L3 ports.

  Higher rate seen on the qos policies attached on the L3 interface which has multicast interest. When the non-rpf packets make way into the node due to wrong handling by the hardware met, the L3 interfaces see these packets wherein they are dropped. But before they get dropped, they get accounted in the egress qos policy on the L3 interface.

  Workaround: Shut the interface on which these non-rpf packets make way or clear the multicast groups once.

- CSCts37316

  CPU keeps 100% while download and extract IOS(8-9 minutes).

  When the IOS file is downloaded and the .tar file is extracted, the CPU usage reached 100%. The CPU usage remains at 100% for approximately 8-9 minutes.

  Workaround: None.

- CSCtt02018

  L2PT double-commits to 12.2(52)EY03 throttle.

- CSCtr69207

  QoS: Router crashes on removal of service-policy configuration from the interface.

- CSCts10366

  Write Core via FTP causes system crash.

  Have configurations to enable core write to FTP server.

```
exception core-file <core_file_name>
exception protocol ftp
exception region-size 65536
exception dump <ip address>
```

The **write core** command causes a system crash.

Workaround: None.

- CSCts08628

  ME3600x 10G ports multicast storm-control is broken.

  When storm control is configured on the Ten Gig (0/2) interface, it does not drop packets when there is a storm.

  Workaround: None.

- CSCth02989

  When copper SFPs are plugged in, SFF8472 LED process causes high CPU utilization.

  When a large number of copper SFPs are plugged into an me3800x device, only the **sh proc cpu sorted** command shows HIgh CPU utilization (~45%) with SFF8472 process consuming the cycles. This is noticed ONLY when Copper SFPs are plugged onto the device. This caused by slow low-level access to the device.

  Workaround: None. This is caused by slow polling of the (i2c) bus and is only an issue with copper SFPs.

- CSCts47982

  Multicast forwarding rate decreases after configuring max-metric.

  ME3600x have 64SVI + 64PIM + 64 HSRP instance. When the **max-metric** command is configured on ME3600x, the multicast forwarding rate is decreased. Multicast traffic drops on trunk ports with output drops incrementing.

  Workaround: Shut the interface on which non-rpf packets are coming on. Alternatively, change the DR priorities so that multicast forwarding happens only from one of the nodes.

- CSCtr44687

  Disable PCI interface when bringing down the switch before crashing.

- CSCtr62816

  ME3600 switch crashed when configuring the service-policy input.

  ME 3600X series Ethernet Access switch crashed when configuring the service-policy input.

  Workaround: Upgrade to 15.1 and later version of IOS.

- CSCtq98204

  ME3600: Source mac-address of a multicast frame is flapping.

  This issue is seen in ME3600 running 12.2(52)EY1 release.

  Workaround: None.

- CSCtr63114

  CDP disable resets management interface of ME3600.

  An ME3600 resets the interface when disabling CDP using **no cdp enable** command. If the interface is configuring with **no cdp enable** command at bootup, the interface will be down/down.

  Workaround: Shut/no shut the interface or enable cdp to bring the interface up.

- CSCtr03069

  The ME3600/ME3800 system hangs while writing crash information.

The ME3600/ME3800 system may be unresponsive or hang while dumping the crash information after a system crash. A reload of IOS immediately after a previous crash may cause the system to hang at boot up, or lead to garbled output on long running commands, (for example **show memory** command).

Workaround: None.

- CSCtr80397

  REP edge no neighbor with stcn stp can see stp convergence issues.

  In certain conditions when running REP edge with no neighbor, where **rep stcn stp** command is configured a TCN may not be sent to allow STP convergence on the neighbor.

  Workaround: None.

- CSCtr83418

  Interface does not come up when speed is set to 100 Mb/s on GI interface.

- CSCtr87467

  ME3600x Management Port Gig0 stays down/down while opposite side is up/up.

  The Ethernet Management Port Gig0 of a ME3600x may remain in down/down state while the opposite interface is up/up. This has been observed on a ME3600x running 12.2(52)EY2 and 15.1(2)EY.

  Workaround: None. To remedy the situation perform a shut/no shut on Gig0.

- CSCtq83601

  EoMPLS traffic stop after TE tunnel path change.

  EoMPLS traffic does not flow after MPLS TE tunnel path changes after FRR. TE tunnel is used as PW. VC does not flap and label stack looks fine.

  Workaround: Shut/no shut AC interface may recover from problem.

- CSCtr77731

  REP fails periodically on TE port.

  When REP is enabled on TE port, the ME3600x/ME3800x goes to failed state without any trigger.

  Workaround: Shut/No shut is a temporary workaround however the issue occurs again after a day or two.

- CSCtq93371

  Approximately 10 sec multicast duplication occurred when the max-metric is configured.

  R1 and R2 have same cost to multicast source. R1 is AW because of big IP address. Where max-metric is configured on R1, the R1 sends PIM Assert. However, R2 does not send PIM Assert for a while, causing PIM Assert, Multicast duplication to occur.

  Workaround: None.

- CSCtr24751

  ME3600X BGP is flapping every 55hour and 58 mins on GE interface.

  No special conditions appear to cause this issue, just peer BGP neighbor and ingress numbers of BGP route from TenGE.

  Workaround: None.

Open Caveats for Cisco IOS Release 12.2 (52) EY2a

The following caveats are open in Cisco IOS Release 12.2(52) EY2a:

- CSCtn77008

  The management ENET LED Port is not working when link is established. In the switch prompt the management port LED is not glowing though the host is alive and it is able to tftp and download the ios image.

  Workaround: None. However you can ping the host manually to verify it is alive.

- CSCtr09290

  Asserts failure messages are seen on the device. This can result in traffic loss for some of the end-devices on certain VLANs. The issue occurs randomly and may occur a few minutes or a few days after boot up.

  Workaround: None.

- CSCtr12244

  SD LED does not glow in the rommon prompt, even though the SD card is present.

  Workaround: None.

- CSCtr50532

  The link polling status interval is currently constant, at 40ms.

  Workaround: Use the **test platform link_poll set_interval** command to configure the link polling status interval. The range is 40ms to 200ms at interval of 20ms.

Resolved Caveats for Cisco IOS Release 12.2 (52) EY2a

The following caveats have been resolved in Cisco IOS Release 12.2 (52) EY2a:

- CSCto04133

  SYS-2-MALLOCFAIL messages seen on console due to Management Port Failure.

- CSCtf28618

  CPU Hog, when running show int transceiver. When the **show interface transceiver** command is used for the first time after reload, it causes CPU Hog.

- CSCtq94117

  ME3800, STP is enabled on REP ports.

- CSCtq61887

  Unexpected packet drop after routing convergence.

- CSCtr19502

  SFF8472 process is causing CPU HOG. The following message appears after 10 min.

  ```
  %SYS-3-CPUHOG: Task is running for (2246)msecs, more than (2000)msecs (15/9),process =
  SFF8472.
  ```

- CSCtn88873

  Traceback observe at src-asic-nile/nile_adjmgr_l3m.c: 124: get_eaid_idex.

- CSCtr31881

Bring down the forwarding path before writing the crash file.

- CSCtr14230

  ME3800: Equal-Cost-Multi-Path (ECMP) Load balancing does not work with Xconnect. Traffic through ME3800 may not be handled properly when it has ECMP to the destination.

  Workaround: Downgrade to IOS 12.2(52)EY1.

- CSCtr25016

  Send break should be disabled by default.

Open Caveats for Cisco IOS Release 12.2 (52) EY2

The following caveats are open in Cisco IOS Release 12.2 (52) EY2:

- CSCto36103

  OSMGR-3-LABEL_EXHAUST issue while attaching egress policy with 4k class.

- CSCto52930

  ME3800x: Incorrect hardware programming for MPLS traffic.

- CSCto64774

  STP and UDLD does not work in QnQ tunnel on ME3600X After reconfiguration.

- CSCtq31562

  Xconnect traffic is down as wrong label is being used by forwarding.

- CSCtj18426
  With IGMP snooping, forwarding does not happen for few entries.

- CSCtj43974

  Secure address count is not correct when mac security max addr config as 1.

- CSCtj50739

  Changing SH group may cause crash if a secure efp is in violation.

- CSCtj83932

  Shaping counters are incorrect on Egress QoS policy.

- CSCtl20118

  CPU hog messages seen on dynamic modification of qos policy.

- CSCtn20598

  Chunk mem leak on 3600/3800X [Niles Stats Ma, NILE EMAPD CHU, fi_handle_t].

- CSCtn25367

  Memory leak observed @ classmap_attach_filter_struct, filter_malloc.

- CSCtf02910

  OPM:IP Packets punted to CPU for routing are not being marked.

- CSCtf19721

  OPM: classification does not work in POP forwarding operation.

- CSCto55216

Routing table change leads to a milli-second-order packet loss.

- CSCto59261

  Unable to modify xconnect configuration on hitting the scale limit.

- CSCto61243

  Platform assert failures on flapping ten gig intf with ebgp sessions.

- CSCti42740

  HSRP configs when config replaced show tracebacks.

- CSCto88017

  Tracebacks upon removing MPLS TE Auto Tunnel configs.

- CSCtq21477

  ME3800X problems with Multicast Traffic.

- CSCti64873

  Switch is inaccessible on reloading box with 1000 EFP QoS configuration.

Resolved Caveats for Cisco IOS Release 12.2 (52) EY2

The following caveats have been resolved in Cisco IOS Release 12.2 (52) EY2.

- CSCtq42245

  Egress classification does not work if the same dscp is set on ingress marking.

- CSCtq06435

  Traffic does not flow over EVC till mac-address table is cleared.

- CSCti33534

  "no ipv6 address autoconfig" may cause crash after router advert. flood.

- CSCtk34115

  Fix sh int null0 display on switch.

- CSCti25339

  SNMP Walk against a VLAN indexed OID causes crash k_dot1dStpPortEntry_get.

- CSCtl44631

  Increase the number of IPv4 routes supported on ME3600.

- CSCtd10712

  NAT: Crash with LDAPv3 traffic.

- CSCsw77313

  Failed authentication with login command changes the logged user.

- CSCth25634

  Password prompted twice for AUTHEN that is falling over to line password.

- CSCtl58877

  Fix CSCti33534 in v122_52_ey_throttle.

- CSCtl43901

Continuous Link syslog messages on Mgmt interface, with dhcp configured.

- CSCtn06092

  Configure prep-commit to include me360x* and me380x* images of v122_52_.
- CSCti00415

  Hump crashes when switch mpls from routed to vlan with 2K vpns.
- CSCtn38836

  TCAM parity error seen on a few RMA units during POST.
- CSCtn24863

  ME3800: SW does not support DOM on Finisar SFP+ 10GE ER.
- CSCtn07021

  VRF aware feature does not work on ME3600X.
- CSCtl51979

  SFP module status is missing in show commands.
- CSCtn45822

  Adding more than 75 HSRP groups throws error.
- CSCtn92643

  Link is not coming up if 1G SFP inserted in 10G slot on humback.
- CSCtn70634

  Send break should be enabled by default.
- CSCto36014

  Yellow alarm [RYEL bit] is set for E1 mode.
- CSCtn28797

  QoS: Packets from CPU does not get egress classified correctly.
- CSCte17893

  ME3600: Combination speed settings not allowed.
- CSCtn25698

  BFD neighborship fails with ACL.
- CSCtj29177

  System clock cannot drive Output Clock on the switch.
- CSCtn48360

  IGMP snooping does not work after disable -> enable igmp snooping.
- CSCtn38803

  RCOM ME3800 High CPU because of label space on the ASIC is 8K.
- CSCsr68157

  Unknown TLV with U bit of 0 in LDP message was not handled properly.
- CSCto31521

  Policer is not working on tengigabitethernet interface.
- CSCto79613

Switch is not forwarding packets properly with size >1518.

- CSCto71170

  ME3600X is manufactured with identical leading 40 bit mac addresses.

- CSCtn64911

  REP edge nn with stcn stp, mst convergence failed on non rep peer.

- CSCto44497

  QoS marking policy is not working with EVC Etherchannel.

- CSCto98272

  TCAM Array Parity errors are found during POST.

- CSCtl70722

  Classification is broken while doing dynamic change on the policy.

- CSCtk56241

  Crash noticed after ASIC assert error messages.

- CSCtq08751

  ip->tag packets egressing switch are getting punted to host q.

- CSCto73371

  Ethernet Service Instance Counters are not updated after shut/no shut.

- CSCto88068

  Manipulating a policy-map causes ME3800 to crash.

- CSCtn84468

  ME360x crashes when polling dot1dTpFdbEntry_get.

- CSCth08845

  Server crashes while generating TGN packets from client.

- CSCto99555

  Platform assert errors on flapping te frr tunnels multiple times.

- CSCsz83592

  7600/IO memory fragmentation - SYS-2-MALLOCFAIL: Memory allocation fail.

- CSCtn98097

  QoS labels are not removed when classes are deleted dynamically.

- CSCtn14387

  Multicast does not work over SVI based EoMPLS with TE tunnels.

- CSCtj49127

  CFM transparency over SVI Eompls broken.

- CSCtq14467

  Traffic stops on HSRP active interface after reload (sometimes).

- CSCto73823

  Ping from standby HSRP router and host to HSRP virtual IP fails.

- CSCtl90499

Packets wrongly get classified after dynamic modification in RWN--Trunk.

Resolved Caveats for Cisco IOS Release 12.2 (52) EY1c

The following caveats have been resolved in Cisco IOS Release 12.2(52)EY1c.

- CSCtn38836

  TCAM parity error is seen on some RMA units during POST, and the following error is set.

  POST: Port ASIC CAM Subsystem Tests: Begin

  TCAM APErr is set

  POST: Port ASIC CAM Subsystem Tests: End, Status Failed

  The subsequent action is a crash, and the unit never boots up.

- CSCto98272

  TCAM Array Parity errors are found during POST. The POST fails the Port ASIC CAM Subsystem Tests, due to TCAM ArrayParity error. This happens during power cycle and does not usually happen on subsequent reloads.

  The following error is set on POST:

  POST: Port ASIC CAM Subsystem Tests: Begin

  TCAM APErr is set

  POST: Port ASIC CAM Subsystem Tests: End, Status Failed

  Subsequent action is a crash, and the unit never boots up.

Resolved Caveats for Cisco IOS Release 12.2 (52) EY1b

The following caveats have been resolved in Cisco IOS Release 12.2 (52) EY1b.

- CSCto79613

  Packets with size greater than 1518 are not forwarding. When this happens, the system may not be able to send or receive any more packets.

- CSCto71170

  ME3600X is manufactured with identical leading 40 bit mac addresses. The problem occurs if the switch base mac addresses have identical leading 40 bit mac addresses. If two ME3600X switches with identical leading 10 hex digits / 40 bits base mac address are directly connected they black hole traffic when the source mac of the traffic is from the switch base mac.

- CSCtk34115

  The null0 interface counters are not updated. Packet counters do not increment. The **show platform ip unicast statistics** command can be used to check the packet counts.

- CSCtl44631

  Increase the number of IPv4 routes supported on 3600. Currently this number is 20k ipv4 routes. This needs to be increased to 24k ipv4 routes. This can be done by taking up TCAM space from ipv6. Presently 5 TCAM blocks are reserved for ipv6 (10k ipv6 routes) and 5 blocks for ipv4 (20k ipv4 routes). This is changed to 4 blocks for ipv4 (8k ipv6 routes) and 6 blocks for ipv4 (24k ipv4 routes).

Resolved Caveats for Cisco IOS Release 12.2 (52) EY1

The following caveats have been resolved in Cisco IOS Release 12.2 (52) EY1.

- CSCtk05868

  When the Resilient Ethernet Protocol (REP) Link Status Layer (LSL) age timer is configured to 120 msec (implying the REP LSL hello timer is 40 msec at a retry of 3), the REP links flap occasionally.

- CSCtk54790

  When the user connects a Dell laptop through the console cable, the ME 3600X switch reloads.

- CSCtk67433

  In the presence of QoS Policy on the Ethernet Virtual Circuit (EVC), when the traffic rate goes beyond the QoS Policy, the Hot Standby Router Protocol (HSRP) packets could get dropped leading to protocol flaps.

- CSCtj79856

  When a class is dynamically removed from a child level (logical) policy and reattached, COS packets are incorrectly classified on the class.

- CSCtk62499

  When the number of unique next hop hosts learned by the system exceeds the system internal limit for Layer 2 rewrite entries, software forwarding kicks in due to incomplete adjacency.

- CSCtk67315

  Under certain combination of EVC/Switched Virtual Interface (SVI), Cisco Discovery Protocol (CDP) packets are not tunneled correctly.

- CSCtl18065

  When an attempt is made to reduce the REP LSL AGE timer below the current default value of 920 msec, the configuration is rejected.

- CSCtc41469

  When user breaks the auto booting of IOS image via Send break, a *** line too large *** message is displayed. This is just a warning message and is not an issue when the extra input characters are simply dropped.

- CSCtl18487

  No POST support for mini IOS image.

Open Caveats for Cisco IOS Release 12.2 (52) EY and Cisco IOS Release 12.2 (52) EY1

Cisco IOS Release 12.2 (52) EY and Cisco IOS Release 12.2 (52) EY1 contain these open caveats:

- CSCtf02910

  Packets sent to the CPU for any reason after ingress quality of service (QoS) processing and then sent out of another port are not classified correctly at egress QoS, and are not remarked per the configured input QoS **set** action.

  Workaround: None

- CSCtf19721

  When you configure egress QoS, matching the outer class of service (CoS) value does not work at the egress provider edge when the egress port is configured as an EoMPLS vc type 4 xconnect (short-pipe model). When the MPLS tag is popped at the egress provider edge, the VLAN tag is exposed, and you cannot match the outer CoS value in this VLAN tag. Packets are put in the CoS 0 class or the class-default class.

  Workaround: Use the pipe model instead of the short pipe model for the provider edge egress port. At the egress edge, configure QoS to **match mpls exp**. Configure **set qos-group** at the ingress and then match on the QoS group at the egress interface.

- CSCth02989

  When you insert a large number of copper SFPs into a switch, a significant percentage of CPU processing cycles are used polling the SFP link status. The percentage is proportional to the number of copper SFPs used. The maximum CPU bandwidth processing copper SFPs is approximately 25 percent of the total CPU bandwidth.

  Workaround: None.

- CSCth03032

  When you configure static IGMP group entries on a switched virtual interface (SVI) on a switch that has multicast routing enabled with source-specific multicast (SSM) group default settings, multicast data traffic is not forwarded from the SVI.

  Workaround: Toggle the state of the SVI interface by entering the **shutdown** command followed by the **no shutdown** command to ensure that the static group entry (s,g) is installed after the (*,g) entry is installed, which is the correct order.

- CSCth06629

  When a policy-map is applied to an EtherChannel member port that is forwarding traffic, if the member port (for example, GigabitEthernet 0/1) is shut down, the output from the **show policy-map interface GigabitEthernet 0/1** privileged EXEC command shows that the output counters are still incrementing.

  Workaround: None. The counters increment even when the EtherChannel member port is shut down.

- CSCth92499

  If you have configured a VRF IP DHCP pool relay destination by using the **vrf** and **relay destination** *ip-address* DHCP pool configuration mode commands, the relay destination line is removed from the configuration when you reload the switch.

  Workaround: Edit the configuration file before rebooting to move the VRF definition before the ip dhcp pool entry.

  For example, in the configuration below, move the ip vrf vrf1 configuration above the ip dhcp pool pool-vrf configuration entry.

```
ip dhcp pool pool-vrf
   vrf vrf1
   relay source 105.0.0.0 255.0.0.0
   relay destination 121.0.0.2
!
!

ip vrf vrf1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
```

- CSCth92486

  A traceback message might appear when you configure a DHCP session with an IP unnumbered interface for the relay agent.

  Workaround: None. This is a temporary traceback condition that does not affect traffic.

- CSCti42740

  If you configure an Ethernet flow point (EFP) on an interface by configuring a service instance, bridge-domain, and VLAN and save the configuration, if you then enter the **config replace flash: default.cfg** privileged EXEC command with the default configuration (no service instance configured), traceback messages appear.

  Workaround: None. Functionality is not affected.

- CSCti54012

  In a ring topology (or a topology with a loop), when you clear dynamic entries in the MAC address table, you might see MAC address flapping on interfaces in the loop that meet these all of these conditions:

  – The interfaces have untagged service instances in the same bridge-domain.

  – The interfaces are running multiple spanning tree (MST) for loop avoidance.

  – The interfaces have keepalive enabled.

  Workaround: Use one of the following workarounds:

  – Configure each untagged service instance on an interface with keepalives enabled in a different bridge-domain.

  – Disable keepalive on interfaces with untagged service instances in the same bridge-domain that are connected in a loop and are running MSTP.

- CSCti59597

  The MPLS VC receive byte counters include the 14-byte Ethernet header in the byte statistics calculations, which adds an additional 14 bytes per packet. The send byte counters might be inaccurate by 4 bytes per packet by not properly accounting for the VLAN tag.

  Examples:

  Receive byte count:

```
Switch# show mpls l2 vc 1400 detail | begin vc statistics
  VC statistics:
    packet totals: receive 1000, send 0
    byte totals:   receive 142000, send 0 <--- The packet size is 142 instead of 128
    packet drops: receive 0, send 0
```

  Send byte count:

```
Switch# show mpls l2 vc 1400 detail | begin VC statistics
  VC statistics:
    packet totals: receive 0, send 1000
    byte totals:   receive 0, send 128000  <-- The packet size should be 124
    packet drops:  receive 0, send 0
```

  Workaround: None. However, the bytes may be manually subtracted or added based on the total packets sent or received.

- CSCti64873

  When you have configured service policies on a very large number of egress EFPs in different bridge domains, the system is unresponsive while the configuration is being applied. The length of time the system is unresponsive varies depending on the number of entries per policy and the TCAM resources. The delay is less for EFPs in the same bridge domain and there is no notable delay for ingress EFPs.

  Workaround: None.

- CSCti68215

  When you are upgrading the software, if you use TFTP/FTP to copy the switch image into flash memory, the process brings the CPU utilization to 90 percent.

  Workaround: None. The cause is a slow flash file system. Routing and switching functionality and high priority traffic processing are not affected.

- CSCti95134

  On a switch with AAA enabled, if you continuously and quickly enter **show** commands, the Ethernet management port appears to freeze up until you stop entering commands.

  Workaround: None required. The problem does not occur when you enter commands at a normal rate.

- CSCti95543

  If you modify the maximum transmission unit (MTU) on a port that is a member of an EtherChannel, the port might not come up even when the configured MTUs are the same on both the member port and the EtherChannel.

  Workaround: Always configure the EtherChannel MTU first and then add the physical port to the port channel. To recover from the condition, shut down and then enable the port by entering the **shutdown** followed by the **no shutdown** interface command on the port.

- CSCtj18426

  In a Resilient Ethernet Protocol (REP) ring environment, when the number of learned IGMP snooping entries is more than the license-supported limits, the forwarding bandwidth decreases for multicast traffic. Forwarding bandwidth remains acceptable when the license limits are not exceeded.

  Workaround: Limit the number of IGMP snooping learned entries to be within the limits supported for the platform license.

- CSCtj21588

  When you have configured the Cisco Network management System (CNS) also referred to as Cisco IOS Configuration Engine, on both the customer edge server and on the switch with an associated template, if you overwrite the startup configuration with the CNS template, the **show startup-config** command output is not correct.

  For example, if you enter a configuration template on the customer edge server with this one line of configuration:

  ```
  Router(config)# cns trusted-server all-agents 1.1.1.1
  ```

  Then associate the device with the this template and configure the switch for CNS where ip-address is the IP address of the Configuration Engine server:

  ```
  Switch(config)# cns trusted-server all-agents ip-address
  Switch(config)# cns event ip-address
  ```

If you enter the **cns config retrieve** *ip-address* **overwrite-startup** privileged EXEC command to overwrite the startup configuration with the configuration template from the server, the startup configuration is corrupted and the **show startup-config** privileged EXEC command output includes extraneous raw hex values and memory address space information as in this example:

```
Switch# show startup-config
Using 43 out of 1572864 bytes00000000:  0A636E73 20747275 73746564 2D736572 .cns
trusted-ser
00000010:  76657220 616C6C2D 6167656E 74732031    ver  all- agents 1
00000020:  2E312E31 2E310A65 6E640AXX XXXXXXXX    .1.1 .1.end.X XXXX
```

Workaround: None.

- CSCtj22513

  When an EtherChannel port channel contains many EFPs with MPLS running on many interfaces, if you set a 10-Gigabit port to the default setting and then enter the **switchport trunk allowed vlan** interface command to allow VLANs, an occasional traceback message appears.

  Workaround: None.

- CSCtj27401

  When the number of BGP routes configured on a switch exceeds the number supported by the installed license and the switch runs for many hours, flapping might occur on VLAN interfaces with an error message similar to this:

  %UTIL-3-IDTREE_TRACE: PW freelist DB:Duplicate ID free for 16785

  Workaround: None. The system automatically recovers with marginal traffic loss.

- CSCtj29087

  When Synchronous Ethernet (SyncE) is running in 2048KHz (nonframing) mode, if the switch loses its line sources and is in holdover or free-run state, it is not able to notify the Synchronization Supply Unit (SSU) that it has lost the line sources. This could result in the switch lower quality clock driving the high quality SSU clock.

  Workaround: None.

- CSCtj29177

  SyncE implementation on the switch does not support the option of the system clock (T0) driving the output clock (T4). Therefore, you cannot use the switch for these functions that are available in other platforms that support BITS OUT:

  - Monitoring the G.8262 Synchronous Equipment Timing Generator (SETG) output for on-site probe for long term measurement.
  - Ethernet Equipment Clock (EEC) feeding the System Equipment Clock (SEC) when there is no SSU on the site (distributing timing on a site between Ethernet and SDH equipment).

  Workaround: None

- CSCtj29340

  When the switch is in SyncE holdover or free-run state, if no inputs are configured for output clock (BITS OUT) or if the input configurations for output clock are removed, the switch could drive the high quality SSU clock with its lower quality clock.

  Workaround: None.

- CSCtj43917

  If you change the encapsulation type on an existing service instance that is routing traffic, the Layer 3 multicast traffic flow stops until the existing multicast route entries are cleared.

Workaround: Enter the **clear ip mroute** privileged EXEC command to clear and relearn the entries in the database to resume traffic forwarding.

- CSCtj43966

  When an SFP-10GBase-CUxM SFP+ module is inserted in the switch, the correct vendor object ID (OID) is not displayed in the ANA network management tool.

  Workaround: None. Functionality is not affected.

- CSCtj43974

  On a secure EFP in protect or restrict violation mode, if you enter the **no mac security maximum addresses** or the **mac security maximum addresses** *value* service-instance configuration command to decrease the MAC security maximum address count, new addresses cannot be learned. All secure addresses are removed as expected, but the violation mode is not disabled.

  Workaround: Use one of these workarounds:

  – Disable MAC security on the EFP, increase the maximum number of secure MAC addresses on the EFP, and then reenable MAC security by entering these service-instance configuration commands:

    no mac security

    mac security maximum addresses *value*

    mac security

  – Change the maximum number of secure MAC addresses on the EFP to x by entering the **mac security maximum addresses** *x-1* followed by the **mac security maximum addresses** *x* service-instance configuration command.

- CSCtj46901

  The minimum REP Link Status Layer (LSL) age-timer value is 920 ms.

  Workaround: None.

- CSCtj47078

  If the switch learns more routes than the installed license supports, CPU hog messages can appear and the switch can become unstable.

  Workaround: Do not allow the switch to learn more routes than the license supports. You can restrict the number of routes that can be learned per VPN routing and forwarding (VRF) instance by entering the **maximum routes** *value* command in IP VRF configuration mode.

- CSCtj48143

  When a GigabitEthernet port operating at 10 or 100 MB/s is in half-duplex mode, the link partner sends many more packets than it receives because the ME3800X and ME 3600X Carrier Sense Multiple Access with Collision Detection (CSMA/CD) backoff is too passive.

  Workaround: None.

- CSCtj50739

  If a secure EFP is in restrict or protect violation mode, changing the split horizon group of another EFP in the same bridge-domain can cause unpredictable system behavior.

  Workaround: Do not change the bridge-domain split-horizon group of an EFP if there is a secured EFP in same bridge-domain in MAC security restrict or protect violation mode.

- CSCtj57866

  In a REP ring configuration with multicast traffic, if you enter the **no rep segment** *segment-id* **edge no-neighbor primary** interface configuration command followed by a **shutdown** command on the interface, a traceback message appears with an OUTOFRANGE message, similar to this one for each VLAN that is configured.

  ```
  %BIT-4-OUTOFRANGE: bit 0 is not in the expected range of 1 to 1015
  ```

  Because the port is shut down and the REP configuration removed, functionality is not affected.

  Workaround: To avoid traceback messages, shut down the interface first and then remove the REP edge port configuration on the interface.

- CSCtj60084

  When the configured Bidirectional Forwarding Detection (BFD) aging time is low, occasional BFD flaps might occur.

  Workaround: Enter the **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value* interface configuration command and configure the **min_rx** to at least 300 ms, which sets the aging time to 900 ms or more and eliminates the BFD flaps.

- CSCtc39766

  In interface configuration mode, the **fair-queue**, **priority-group** and **random-detect** commands are duplicated.

  Workaround: None.

- CSCte17893

  When using a copper interface in the GigabitEthernet port on the ME 3800X or ME 3600X-24FS, the interface configuration commands **speed auto 10**, **speed auto 100**, or **speed auto 1000** will return the error message:

  ```
  Speed autonegotiation subset is not supported on this interface
  ```

  Workaround: None.

- CSCti83257

  When the **clear mac address-table dynamic** command is executed, both learned and configured sticky MAC addresses are removed from the MAC address table.

  Workaround: To delete only dynamically learned non-sticky and non-permit addresses, use one of these two commands:

  - **clear ethernet service instance id interface mac table [***hhhh.hhhh.hhhh***]**
  - **clear bridge-domain mac table**

- CSCtj35054

  When the ME 3600X or ME 3800X is deployed as a multicast-edge router, and the state of the multicast routing is toggled using the **ip multicast-routing** command. traffic forwarding is stopped.

  Workaround: After disabling multicast routing using the **ip multicast-routing** command, use the **clear ip multicast-route** command to clear the state of the IOS mroute database, before re-enabling multicast routing using the **ip multicast-routing** command.

- CSCtj38270

  Ethernet Local Management Interface Provider Edge (ELMI-PE) functionality is not supported.

  Workaround: None.

- CSCtj49127

  Connectivity Fault Management (CFM) transparency over SVI EoMPLS is not supported. CFM frames transported over SVI EoMPLS are dropped.

  Workaround: Disable CFM globally on the switch.

- CSCtj63232

  When an interface is reset to default using the **default interface** command, the STP state may switch from FWD to BLK and the interface may restart.

  Workaround: None.

- CSCtj66151

  Multicast traffic is forwarded to an interface when storm control action is set as trap.

  Workaround: Remove the storm control action trap from the configuration.

- CSCtj66619

  When multicast storm-control is enabled on a Layer 2 port which is a member of a Layer 3 SVI interface with pim dense-mode enabled, multicast traffic is forwarded.

  Workaround: None.

- CSCtj83932

  When a QoS shaping policy is applied to an interface, and the interface becomes congested, the output from the **show policy-map interface** command displays a higher shaping rate than the configured shaping rate.

  Workaround: Issue the **show policy-map interface** command with an interval of 3 minutes (with load-interval of 30 sec on the interface). The output of the command then displays the correct shaping rate.

- CSCtj94124

  When ME 3800X box was in operation an exception was seen following few error messages related to bad enqueue/refcount.

  Workaround: None.

- CSCtj97102

  A high CPU rate is observed when tunnelling through a ME 3600X or ME 3800X switch.

  Workaround: Reconfigure the tunnel configuration.

- CSCtk34689

  Counters displayed using the **show interface Null0** command are not incremented.

  Workaround: Use the **show platform ip unicast statistics** command to display current values for the counters.

- CSCtk56241

  When there is an update relating to an old MAC address (e.g. switch learns a MAC address again). assert failures are seen after the MAC address change.

  Workaround: None.

- CSCtk67412

  Upon node reload, the **ip routing protocol purge interface** command is automatically removed from the configuration.

  Workaround: Add **ip routing protocol purge interface** command after router reload.

Related Documentation

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

ME 3800X switch:
http://www.cisco.com/en/US/products/ps10965/tsd_products_support_series_home.html

ME 3600X switch:

http://www.cisco.com/en/US/products/ps10956/tsd_products_support_series_home.html

Note Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the "Configuring the Switch with the CLI-Based Setup Program" appendix in the hardware installation guide.
- For upgrading information, see the "Downloading Software" section in the release notes.

- *Cisco ME 3800X and ME 3600X Switch Software Configuration Guide*
- *Cisco ME 3800X and ME 3600X Switch Command Reference*
- *Cisco ME 3800X and ME 3600X System Message Guide*
- *Cisco ME 3800X and ME 3600X Switch Hardware Installation Guide*
- *Cisco ME 3800X and ME 3600X Switch Getting Started Guide*
- *Installation Notes for the Cisco ME 3800X and ME 3600X Switch Power-Supply and Fan Modules*
- *Regulatory Compliance and Safety Information for the Cisco ME 3800X and ME 3600X Switches*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Notes*

These 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

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
- *Cisco CWDM SFP Transceiver Compatibility Matrix*
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

---

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