



# Release Notes for the Cisco ME 3800X, ME 3600X and ME 3600X-24CX Switch, Cisco IOS Release 15.2(4)S and Later Releases

---

**Last Updated: August 14, 2014**

These release notes include important information about the following Cisco IOS releases that run on the Cisco ME 3800X, ME 3600X and ME 3600X-24CX switches:

- Cisco IOS Release 15.2(4)S
- Cisco IOS Release 15.2(4)S1
- Cisco IOS Release 15.2(4)S2
- Cisco IOS Release 15.2(4)S3
- Cisco IOS Release 15.2(4)S4
- Cisco IOS Release 15.2(4)S6

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 7.
- 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 7.

For the complete list of Cisco ME 3800X, ME 3600X and ME 3600X-24CX switch documentation, see the “[Related Documentation](#)” section on page 34.

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=http://www.cisco.com/cisco/web/download/index.html#rpm>



# Contents

- [“Hardware Supported” section on page 2](#)
- [“Software Licenses and Features” section on page 3](#)
- [“Upgrading the Switch Software” section on page 7](#)
- [“Installation Notes” section on page 11](#)
- [“New Software Features” section on page 11](#)
- [“Important Note” section on page 14](#)
- [“Open and Resolved Caveats” section on page 14](#)
- [“Related Documentation” section on page 34](#)
- [“Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page 35](#)

## 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.
Cisco ME-3600X-24CX-M	<p><b>IO mode 1</b></p> <p>16 Gigabit Ethernet SFP downlink ports, 8 SFP/copper downlink ports and 2 XFP (10 Gigabit) uplink ports;16 T1/E1 interfaces; supports removable, hot-swappable AC and DC input power supply and fan modules.</p> <p><b>IO mode 2</b></p> <p>8 SFP/copper downlink ports and 4 XFP (10 Gigabit) uplink ports;16 T1/E1 interfaces; supports removable, hot-swappable AC and DC input power supply and fan modules.</p>
SFP+ modules	SFP-10GE-SR, SFP-10GE-LR, SFP-10GE-LRM, SFP-H10GB-CUxM, SFP-10G-ER, SFP-10G-ZR

**Table 1** Supported Hardware (continued)

Device	Description
SFP+ modules supported on ME3600X-24TS, ME3600X-24FS, and ME3800X	SFP-10GE-SR, SFP-10GE-LR, SFP-10GE-LRM, SFP-H10GB-CU <sub>x</sub> M, SFP-10G-ER, SFP-10G-ZR, DWDM-SFP10G-61.41, DWDM-SFP10G-60.61, DWDM-SFP10G-59.79, DWDM-SFP10G-58.98, DWDM-SFP10G-58.17, DWDM-SFP10G-57.36, DWDM-SFP10G-56.55, DWDM-SFP10G-55.75, DWDM-SFP10G-54.94, DWDM-SFP10G-54.13, DWDM-SFP10G-53.33, DWDM-SFP10G-52.52, DWDM-SFP10G-51.72, DWDM-SFP10G-50.92, DWDM-SFP10G-50.12, DWDM-SFP10G-49.32, DWDM-SFP10G-48.51, DWDM-SFP10G-47.72, DWDM-SFP10G-46.92, DWDM-SFP10G-46.12, DWDM-SFP10G-45.32, DWDM-SFP10G-44.53, DWDM-SFP10G-43.73, DWDM-SFP10G-42.94, DWDM-SFP10G-42.14, DWDM-SFP10G-41.35, DWDM-SFP10G-40.56, DWDM-SFP10G-39.77, DWDM-SFP10G-38.98, DWDM-SFP10G-38.19, DWDM-SFP10G-37.40, DWDM-SFP10G-36.61, DWDM-SFP10G-35.82, DWDM-SFP10G-35.04, DWDM-SFP10G-34.25, DWDM-SFP10G-33.47, DWDM-SFP10G-32.68, DWDM-SFP10G-31.90, DWDM-SFP10G-31.12, DWDM-SFP10G-30.33
SFP modules	GLC-FE-100FX, GLC-FE-100EX, GLC-FE-100ZX, GLC-FE-100LX, GLC-FE-100BX-U, GLC-FE-100BX-D, GLC-LH-SM, GLC-SX-MM, GLC-EX-SMD, 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, SFP-GE-L, SFP-GE-S, SFP-GE-T, DWDM-SFP-xx
SFP modules supported on Cisco ME-3600X-24CX	GLC-FE-100FX-RGD, GLC-FE-100LX-RGD, GLC-LX-SM-RGD, GLC-SX-MM-RGD, GLC-ZX-SM-RGD, GLC-BX-U, GLC-BX-D, and GLC-EX-SMD
XFP modules supported on Cisco ME-3600X-24CX	XFP-10G-MM-SR, XFP-10GLR-OC192SR-RGD, XFP-10GER-OC192IR-RGD, XFP-10GZR-OC192LR-RGD, XFP-10GZR-OC192LR, XFP-10GER-192IR-L, XFP-10GLR-192SR-L, DWDM-XFP-C
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 5](#).

The ME3600X-24CX supports the above licenses plus:

- 10G license
- 1588BC license
- T1/E1 counted license

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 license.
- Metro IP services 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 6](#).

To install a software image, see the “[Upgrading the Switch Software](#)” section on [page 7](#) 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/partner/docs/ios/csa/configuration/guide/csa\\_commands.html](http://www.cisco.com/en/US/partner/docs/ios/csa/configuration/guide/csa_commands.html)

An emergency evaluation license is embedded in the software image and does not require the installation of a license file. Specify which evaluation license to enable by using the **license boot level** command.

Enabling evaluation license on an ME 3800X:

```
ME3800X# configure terminal
ME3800X(conf)# license boot level <MetroEthServices|MetroIPServices|MetroAggrServices>
```



**Note** Only MetroAggrServices is supported during evaluation. Accept the EULA.

```
ME3800X(conf)# exit
ME3800X# write memory
ME3800X# reload
Note: This evaluation license will be validated only after reload.
```

Enabling evaluation license on an ME 3600X:

```
ME3600X# configure terminal
ME3600X(conf)# license boot level <MetroIPAccess|AdvancedMetroIPAccess>
```



**Note** Only AdvancedMetroIPAccess is supported during evaluation. Accept the EULA.

```
ME3600X(conf)# exit
ME3600X# write memory
ME3600X# reload
Note: This evaluation license will be validated only after a reload.
```

After entering the **license boot level** command, you are prompted to accept the End-User Licensing Agreement (EULA). After accepting the EULA, exiting configuration mode, and saving the running configuration to memory, reload the switch to apply the evaluation license.



**Note** The evaluation period is valid for 60 days. When the 60 day evaluation period ends, the evaluation license is unusable after the next reload.

Upon installation of a license file, the license automatically updates to the new license type. There is no need to clear the evaluation license.

**Table 2** *ME 3600X Supported Features per License*

<b>Metro IP Access (Universal Image)</b>	<b>Advanced Metro IP Access license</b>
<ul style="list-style-type: none"> <li>• Basic Layer 2 features (including 802.1Q)</li> <li>• Ethernet Virtual Circuits (EVCs)</li> <li>• IPv4 routing—RIP, OSPF, EIGRP, IS-IS, and BGP</li> <li>• Bidirectional Forwarding Detection (BFD)</li> <li>• Multicast routing —PIM, DM, SSM, and SSM mapping</li> <li>• Ethernet Operations, Administration, and Maintenance (OAM)—802.1ag, 802.3ah, and E-LMI</li> <li>• Multiple Spanning Tree Protocol (MSTP), Resilient Ethernet Protocol (REP), and Flex Links</li> <li>• Synchronous Ethernet with Ethernet Synchronization Messaging Channel (ESMC)</li> <li>• Multi VRF-CE (VRF-Lite) with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)</li> <li>• Switch Database Management (SDM) templates</li> </ul>	<ul style="list-style-type: none"> <li>• All features in the Metro IP Access image</li> <li>• Multiprotocol label switching (MPLS)</li> <li>• MPLS traffic engineering and Fast Reroute</li> <li>• MPLS OAM</li> <li>• MPLS VPN</li> <li>• Ethernet over MPLS (EoMPLS)</li> <li>• Pseudowire redundancy</li> <li>• Virtual Private Lan Service (VPLS)</li> </ul>

**Table 3** *ME 3600X License Scaling and Template*

<b>Supported feature</b>	<b>Metro IP Access</b>		<b>Advanced Metro IP Access</b>		
	<b>Default</b>	<b>IPv4</b>	<b>Default</b>	<b>IPv4</b>	<b>Application template</b>
SDM Templates					
MAC addresses	8 K	8k	16 K	16 K	16 K
IPv4 routes	20 K	24K	20 K	24 K	12 K
IPv6 routes	5 K	4 K	5 K	3 K	4 K
Multicast groups	1 K	1 K	1 K	1 K	1 K
Bridge domains	4 K	4 K	4 K	4 K	4 K
ACL entries	2 K	2 K	2 K	2 K	IPv4: 2 K IPv6: 1 K
IPv4 QoS classification	4 K	4 K	4 K	4 K	1 K

**Table 4** *ME 3800X Supported Features per License*

Metro Ethernet Services (Universal Image)	Metro IP Services license	Metro Aggregation Services license
<ul style="list-style-type: none"> <li>Basic Layer 2 features (including 802.1d and 802.1Q)</li> <li>EVCs</li> <li>Ethernet OAM—802.1ag, 802.3ah, and E-LMI</li> <li>MST, REP, Flex Links</li> <li>Synchronous Ethernet with Ethernet Synchronization Messaging Channel (ESMC)</li> </ul>	<ul style="list-style-type: none"> <li>All features in the Metro Ethernet Services image</li> <li>IPv4 routing—RIP, OSPF, EIGRP, IS-IS, and BGP</li> <li>BFD</li> <li>Multicast routing—PIM, DM, SSM, and SSM mapping</li> <li>Multi VRF-CE with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)</li> </ul>	<ul style="list-style-type: none"> <li>All features in the Metro IP Services license</li> <li>MPLS</li> <li>MPLS traffic engineering and Fast Reroute</li> <li>MPLS OAM</li> <li>MPLS VPN</li> <li>EoMPLS</li> <li>Pseudowire redundancy</li> <li>Virtual Private Network (VPLS)</li> </ul>

**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
IPv6 routes	500	500	21 K	40 K	12 K	16 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
IPv4 QoS classification	4 K	4 K	4 K	4 K	4 K	24 K

**Table 6** *ME 3800X Scaled Metro Aggregation Templates*

Supported feature	Scaled Metro Aggregation Service License		
	Default	VPNv4	VPNv4+IPv6
<b>SDM Templates</b>			
MAC table	256 K	256 K	256 K
IPv4 routes	32 K	80 K	80 K
IPv4 routing groups	4 K	8K	2 K
IPv6 routes	16 K	8 K	40 K
Multicast groups	4 K	4 K	2 K
Bridge domains	8 K	4 K	8 K

Table 6 ME 3800X Scaled Metro Aggregation Templates (continued)

Supported feature	Scaled Metro Aggregation Service License		
ACL entries	16 K	4 K	4 K
IPv4 QoS classification	24 K	12 K	12 K

## Upgrading the Switch Software

- “Finding the Software Version and Feature Set” section on page 7
- “Deciding Which Files to Use” section on page 7
- “Installing Software Images and Licenses” section on page 9

## 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 7** Cisco IOS Software Image Files

Filename	Description
me380x-universal-tar.152-4.S.tar me380x-universal-tar.152-4.S1.tar me380x-universal-tar.152-4.S2.tar me380x-universal-tar.152-4.S3.tar me380x-universal-tar.152-4.S4.tar	Cisco ME 3800X universal image.
me380x-universalk9-tar.152-4.S.tar me380x-universalk9-tar.152-4.S1.tar me380x-universalk9-tar.152-4.S2.tar me380x-universalk9-tar.152-4.S3.tar me380x-universalk9-tar.152-4.S4.tar	Cisco ME 3800X universal cryptographic image. This image has the Metro Ethernet features plus Kerberos and SSH.
me360x-universal-tar.152-4.S.tar me360x-universal-tar.152-4.S1.tar me360x-universal-tar.152-4.S2.tar me360x-universal-tar.152-4.S3.tar me360x-universal-tar.152-4.S4.tar	Cisco ME 3600X universal images.
me360x-universalk9-tar.152-4.S.tar me360x-universalk9-tar.152-4.S1.tar me360x-universalk9-tar.152-4.S2.tar me360x-universalk9-tar.152-4.S3.tar me360x-universalk9-tar.152-4.S4.tar	Cisco ME 3600X universal cryptographic image. This image has the Metro IP access features plus Kerberos and SSH.
me360x_t-universal-tar.152-4.S.tar me360x_t-universal-tar.152-4.S1.tar me360x_t-universal-tar.152-4.S2.tar me360x_t-universal-tar.152-4.S3.tar me360x_t-universal-tar.152-4.S4.tar	Cisco ME 3600X-24CX-M universal images.
me360x_t-universalk9-tar.152-4.S.tar me360x_t-universalk9-tar.152-4.S1.tar me360x_t-universalk9-tar.152-4.S2.tar me360x_t-universalk9-tar.152-4.S3.tar me360x_t-universalk9-tar.152-4.S4.tar	Cisco ME 3600X-24CX-M universal cryptographic image. This image has 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 End of Sale and End of Life Products at this URL:

[http://www.cisco.com/en/US/products/sw/iosswrel/prod\\_category\\_end\\_of\\_life.html](http://www.cisco.com/en/US/products/sw/iosswrel/prod_category_end_of_life.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* at this URL:

[http://www.cisco.com/en/US/partner/docs/ios-xml/ios/fundamentals/command/Cisco\\_IOS\\_Configuration\\_Fundamentals\\_Command\\_Reference.html](http://www.cisco.com/en/US/partner/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.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 7 on page 8](#) to identify the file that you want to download.
- Step 2** Locate the software image file:
- If you are a registered customer, go to this URL and log in.  
<http://www.cisco.com/cisco/software/navigator.html?a=http://www.cisco.com/cisco/web/download/index.html#rpm>
  - For ME 3800X, navigate to **Switches > Service Provider Switches - Ethernet Aggregation**.  
For ME 3600X, navigate to **Switches > Service Provider Switches - Ethernet Access**.
  - Navigate to your switch model.
  - 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 enter 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.151-2.EY/me380x-universal-mz.151-2.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 this 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# config t
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

The following sections provides information on new software features:

- [Cisco IOS Release 15.2\(4\)S, page 11](#)
- [Cisco IOS Release 15.2\(4\)S2, page 14](#)

## Cisco IOS Release 15.2(4)S

The following new software features are introduced in Cisco IOS Release 15.2(4)S.

**MPLS-TP Support**—The Multiprotocol Label Switching (MPLS) Transport Profile (TP) feature enables you to create tunnels that provide the transport network service layer over which IP and MPLS traffic traverse. MPLS-TP tunnels enable a transition from Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) time-division multiplexing (TDM) technologies to packet switching to support services with high bandwidth requirements, such as video. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/chassis/configuration/guide/swmp\\_transport\\_profile.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swmp_transport_profile.html)

**6PE Support**—The IPv6 Provider Edge (6PE) feature facilitates provisioning of IPv6 services for the Cisco ME3600X and ME3800X switches. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/sw6vpe.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/sw6vpe.html)

**IPv6 VPN over MPLS (6VPE)**—IPv6 VPN Provider Edge (6VPE) feature provides support for IPv6 VPN services over MPLS core networks. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/sw6vpe.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/sw6vpe.html)

Synthetic Frame Loss Measurement (ETH-SLM)—The Synthetic Frame Loss Measurement (ETH-SLM) feature measures frame loss using synthetic frames, rather than data traffic. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swy1731pm.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swy1731pm.html)

IPSLA Support for ETH-SLM (Ethernet Synthetic Loss Measurement in Y1731)—This feature provides IPSLA Support for ETH-SLM (Ethernet Synthetic Loss Measurement in Y1731). For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swy1731pm.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swy1731pm.html)

BGP 4 bytes ASN—The BGP Support for 4-byte autonomous system numbers (ASN) feature provides support for 4 byte AS numbers in BGP per RFC 4893. For details about this feature see:

[http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\\_bgp/configuration/15-1sg/irg-4byte-asn.html](http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-4byte-asn.html)

BGP Per neighbor graceful restart configuration—The BGP Per neighbor graceful restart configuration feature allows for enabling and disabling Graceful Restart Per BGP Neighbor. For details about this feature see:

[http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\\_bgp/configuration/15-1sg/irg-grace-restart-neighbor.html](http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-grace-restart-neighbor.html)

BGP Support for Dual AS Configuration for Network AS Migration—This feature provides BGP Support for Dual AS Configuration for Network AS Migrations. For details about this feature see:

[http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\\_bgp/configuration/15-1sg/irg-dual-as.html](http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-1sg/irg-dual-as.html)

Table Map QoS—Table Map QoS functionality-Enhancement to existing feature. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swqos.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swqos.html)

VRRP MIB - RFC2787—This feature provides support for RFC2787: "Definitions of Managed Objects for the Virtual Router Redundancy Protocol". For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swvrrp.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swvrrp.html)

BFD-BFD Hardware Offload Support—BFD-BFD Hardware Offload Support-This feature provides support of BFD sessions in ME3600X-24CX hardware supporting offloading of BFD sessions. For details about this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/chassis/configuration/guide/swbfd.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swbfd.html)

Circuit Emulation over Packet Switched Network—The feature provides support for Circuit Emulation over Packet Switched Network feature on Cisco ME3600x-24CX switch. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/chassis/configuration/guide/swpseudowire.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swpseudowire.html)

DAI—DAI (Dynamic ARP Inspection)-DAI is used to verify the sanity of IP to MAC address mappings specified in ARP packets sent by connected hosts or neighboring switches. This prevents man in the middle attacks that can be carried out by poisoning ARP with the help of ARP packets containing invalid IP to MAC address mappings. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swdynarp.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swdynarp.html)

T1/E1 Support—T1/E1 support on ME-3600-24CX-This feature provides support for T1/E1 ports on ME3600C-24CX switch. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_2\\_S/chassis/configuration/guide/sw\\_T1-E1.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_2_S/chassis/configuration/guide/sw_T1-E1.html)

PBR—Policy based routing (PBR) provides a flexible means of routing packets by allowing the user to configure a defined policy for traffic flows. This lessens reliance on routes derived from routing protocols. PBR gives you more control over routing by extending and complementing the existing mechanisms provided by routing protocols. PBR allows you to set the IP precedence. It also allows you to specify a path for certain traffic, such as priority traffic over a high-cost link.

For Cisco ME 3600X, the PBR feature is supported with the application SDM template. For Cisco ME 3800X, the this feature is supported with the scaled license. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swpbr.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swpbr.html)

OSPF TTL Security Check—The OSPF TTL Security Check feature allows the addition of an extra layer of protection to OSPF by setting and checking TTL values. Neighbors will send packets with a TTL of 255 and we will only accept OSPF packets with a 254 TTL. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/configuration/guide/swospf\\_ttl.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/configuration/guide/swospf_ttl.html)

## EVC MIB

The EVC MIB is a Cisco proprietary Simple Network Management Protocol (SNMP) MIB for managing an Ethernet infrastructure. SNMP versions 1 and 2c are supported. The EVC MIB consists of 18 tables and three notifications. The command-line interface (CLI) commands **snmp-server enable traps Ethernet evc** and **snmp-server host traps evc** are implemented for enabling or disabling notifications. Notifications are disabled by default.

Support for service instances such as Layer 2 VLAN interfaces was added in Cisco IOS Release 12.2(33)SRD1. Service instances are represented as subinterfaces in the IF-MIB and associated with an ifIndex. Four commands support this feature: **debug if-mgr trace efp-ext**, **debug if-mgr errors efp-ext**, **snmp ifindex**, and **snmp trap link-status**. The **snmp** commands are supported under service instance configuration mode (config-if-srv). Changes to configurations and existing commands are not required.

To use the EVC MIB, the Ethernet Infrastructure module must be present in the Cisco IOS software image, and Metro Ethernet Infrastructure High Availability must be in place. SET operations are not supported on any object in Cisco IOS Releases 12.2(33)SRD and 12.2(33)SRD1.

For detailed information about EVC MIB-related commands, see the Cisco IOS Carrier Ethernet Command Reference, found here:

<http://www.cisco.com/en/US/partner/docs/ios-xml/ios/cether/command/ce-cr-book.html>

For detailed information about SNMP commands, see both the Cisco IOS Network Management Command Reference, found here:

[http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm\\_book.html](http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html) and the Cisco IOS Interface and Hardware Component Command Reference, found here:

[http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir\\_book.html](http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_book.html)

For detailed information about the EVC MIB, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator, found here:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

## Cisco IOS Release 15.2(4)S2

Cisco ME 3600X 24CX 1588-2008 Boundary Clock—The Cisco ME 3600X 24CX Series Switch supports the Precision Time Protocol (PTP) as defined by the IEEE 1588-2008 standard. PTP provides accurate time synchronization over packet-switched networks. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.2\\_4\\_S/chassis/configuration/guide/swclocking.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.2_4_S/chassis/configuration/guide/swclocking.html)

## Important Note

Switch Port Analyzer (SPAN) is not supported.

## Open and Resolved Caveats

The following section provides information on open and resolved caveats:

- [Open Caveats for Cisco Release 15.2\(4\)S, page 14](#)
- [Open Caveats for Cisco Release 15.2\(4\)S1, page 15](#)
- [Open Caveats for Cisco Release 15.2\(4\)S2, page 18](#)
- [Open Caveats for Cisco Release 15.2\(4\)S3, page 23](#)
- [Open Caveats for Cisco Release 15.2\(4\)S4, page 23](#)
- [Resolved Caveats for Cisco Release 15.2\(4\)S1, page 25](#)
- [Resolved Caveats for Cisco Release 15.2\(4\)S2, page 25](#)
- [Resolved Caveats for Cisco Release 15.2\(4\)S3, page 26](#)
- [Resolved Caveats for Cisco Release 15.2\(4\)S4, page 30](#)
- [Resolved Caveats for Cisco Release 15.2\(4\)S6, page 33](#)

## Open Caveats for Cisco Release 15.2(4)S

- CSCty80541
 

Having EVC BD, with split-horizon group as 0 or 2 as CE-facing, drops the traffic over VPLS core pseudowire (split-horizon enabled).

Conditions: This issue is observed when CE-facing interface is EVC BD with split-horizon group as 0 or 2. For split-horizon group 1, traffic flows fine. The issue with CE-facing as group 0, cannot be fixed because of hardware limitation.

Workaround: There is no workaround.
- CSCtz16798
 

On configuring "ip pim snooping" on a L3 MCAST box, crash is observed.

Conditions: This issue occurs when L2 specific functionality is enabled on a L3 box. This is more of an unsupported and undesired configuration as the L3 box is capable of building the MCAST database on its own.

- Workaround: Do not configure "ip pim snooping" on L3 Cisco ME 3600X and ME 3800X boxes.
- CSCtz74604
 

With a scaled 6PE and 6VPE configuration, a crash is observed.

Conditions: This symptom is observed on flapping the interfaces, and defaulting the configurations with a scaled 6PE and 6VPE configuration.

Workaround: There is no workaround.
  - CSCtz77011
 

Multicast traffic may not be forwarded correctly when traffic is received on a layer 2 port-channel.

The PIM DR forwards traffic onto the layer 2 port-channel, while the other node only has a \*,G entry. In this situation, the traffic is not forwarded out of the layer 2 port with receivers.

Conditions: This issue is observed in a setup with two Cisco ME 3600X with layer 2 port-channel in between and mVPN. This issue is observed only on port-channel 1.

Workaround: Avoid port-channel 1 by creating a dummy port-channel 1 and start using from port-channel 2 until port-channel 126.
  - CSCua31903
 

IPv6 Traffic forwarded to wrong VRF when address is same on both VRFs.

Conditions: When traffic is sent from the VRF1 interface of UPE-1 to 5000::1, the traffic is forwarded over the VRF2 interface of UPE-2. It should be sent over the VRF1 interface on UPE-2.

Workaround: None.
  - CSCua43153
 

ME3800 is corrupting the VLAN information in the packet.

Conditions: The ME3800 acts as an nPE, sending the wrong VLAN tag for a VLAN in the egress direction towards spoke.

Workaround: None.
  - CSua46335
 

OSPF Flaps with RPW.

Conditions: OSPF flaps appear at intervals of around 30 minutes.

Workaround: None.
  - CSCua83876
 

Multicast streams stop being forwarded with message MET FULL ERR.

Some multicast streams may be stopped being forwarded or new multicast streams cannot be joined. When this happens, a MET FULL ERR message appears.

Conditions: This issue is observed on a Cisco ME 3600X running IOS 15.2(2)S1.

Workaround: None. A reboot is required to temporarily clear the situation.

## Open Caveats for Cisco Release 15.2(4)S1

- CSCty31982
 

Port-channel is in a suspended state, with the peer throwing messages that LACP is not enabled on the remote node.

Conditions: This issue is observed upon reload.

Workaround: Remove/add the untagged service instance which has L2peer STP and LACP configured.

- CSCty77616

BGP VPNV4 flaps after reload if BGP peer route is learned via TE.

Upon reloading the Cisco ME 3600X 24CX, its BGP peership with the Cisco ME 3800X comes up, but the peer PE Cisco ME 3800X does not learn any routes from the Cisco ME 3600X 24CX after reloading. Upon expiry of the hold timer on the Cisco ME 3800X, the BGP goes down and comes back up. Again, no routes are learned on the Cisco ME 3800X and the BGP goes down. This happens continually. The same behavior is observed upon reloading the Cisco ME 3800X.

Conditions: All PE (Cisco ME 3600X, Cisco ME 3800X, and Cisco ME 3600X 24CX) have TE tunnels starting from each PE to all other PE. Autoroute announce is configured on all PEs, so PEs are reachable to each other via a TE tunnel. Each PE has VPNV4 peership with all other PEs.

Workaround: Disable the TE tunnel, then after the first flap, the routes are learned and BGP comes up. Then enable TE and BGP remains up. Upon setting IP "ip tcp mss adjust 1200" BGP comes up.

- CSCty82122

Traceback messages are seen at n13mmpd\_adjmgr\_13m\_update\_port\_mcast\_nh

The following traceback message appears:

```
platform assert failure: l3m_port_met->efp.ge_allocated == TRUE:
../src/src-asic/adjmgr_13m.c: 6110: del_l3m_efp_met
-Traceback= 642CF0z 1F2A084z 2062840z 20659F8z 20668A0z 294866Cz 2948D18z 294D780z
29A9300z 29A47C0z
```

Conditions: Specific configuration is loaded and traffic is started.

Workaround: None.

- CSCtz06740

MPLS LSP ping does not work when the PE-to-PE TE tunnel is down.

Conditions: The PE-to-PE tunnel is down, and the next hop to PE1 has TE tunnel to remote PE2, and PE1 is ME3600.

Workaround: None.

- CSCtz58189

The Cisco ME 3600X crashes when using the **config replace** command with certain QoS configurations.

Conditions: When you try to replace the configuration on the router with the configuration that removes the configurations, the router crash occurs.

Workaround: None.

- CSCtz58391

Cisco ME 3600X: Ingress QoS TCAMs are not cleared after certain dynamic changes.

Conditions: Upon removing the encapsulation from the service instance and then deleting the service instance, QoS TCAMs are not cleared.

Workaround: Instead of deleting the encapsulation first, delete the service instance.

- CSCtz60398

Continuous platform asserts failure traceback messages with CFM over Xconnect on the box.



Conditions: This issue occurs with CFM over Xconnect with MPLS TE in core. Flap the core facing link.

Workaround: None.

- CSCtz61032

Xconnect traffic is routed if the MTU exceeds the core MTU, in case of MPLS over SVI.

An IP lookup is done on the xconnect traffic, which should not happen.

Conditions: LS is configured on SVI and the MTU exceeds the core MTU.

Workaround: MPLS over SVI is not supported in the 15.2(4)S releases.

- CSCtz91502

The Cisco ME 3600X and Cisco ME 3800X unicast met shows multiple ReplicationContextQueueEntry and traffic is flooded to all ports in the VLAN.

Conditions: This issue is observed when an access port is in the same VLAN as the rep segment and a rep flap is seen.

Workaround: Clear MAC address table fixes the CQE entries.

- CSCub11348

Broadcast traffic flows over Standby Spoke VC and then gets punted.

Conditions: The traffic comes over the Core VCs and then flows over the Standby Spoke VC from Hub to Spoke. In the Spoke, the traffic received from the Spoke VC gets punted to the CPU (Software Forwarded).

Workaround: None.

- CSCub22049

Native mcast traffic is not forwarded over the Cisco ME 3600X after a core INTF shut/no shut operation.

After the repetitive trigger on mVPN setup on the router (such as core INTF shut/no shut), one of the native multicast streams of terrain is not flowing as expected.

Workaround: None.

- CSCub24496

On the Loopback interface used for BGP neighbor establishment, deleting the "ip pim sparse-mode" and adding back the "ip pim sparse-mode" results in traceback messages. Memory leaks are also observed.

Conditions: This issue has been observed under the following conditions:

- The Cisco ME 3600X is running Cisco IOS Release 15.2(4)S.
- Multicast stream can be received on any type of interface (L2/L3).

Workaround: None.

- CSCub26072

VRF replication is not occurring with the Cisco ME 3600X or Cisco ME 3800X as the VRF RP.

Conditions: This issue has been observed under the following conditions:

- The Cisco ME 3600X is running Cisco IOS Release 15.2(4)S.
- Multicast stream can be received on any type of interface (L2/L3).

- The (S,G) is not hardware programmed for an MSDP created entry (the source is on a VRF1 on N1 and the receiver is on a S1-S2 switch). Core replication is happening but VRF replication is not working properly.

Workaround: None.

- CSCuc13364

Traffic is not flowing out of the GE port on the Cisco ME 3600X.

The egress service policy on EFP is dropping all traffic in egress. The offered rate equals the drop rate. the interface output rate is zero, and the output drop is increasing.

Conditions: This issue is observed on a Cisco ME 3600X running 15.2(2)S.

- CSCub34595

Enabling Dynamic ARP Resolution (DAI) on a VLAN may cause ARP resolution to fail for hosts in other VLANs.

Workaround: Enable DAI for the failing VLAN with IP ARP inspection trust. For example:

```
ip arp inspection vlan 30
int gi 0/10
 ip arp inspection trust
int gi 0/11
 ip arp inspection trust
```

- CSCubm98385

CFM over Xconnect remote MEPs are not learned.

Conditions: Have CFM over Xconnect on the Cisco ME 3600X and TE tunnels in the core. Core link is mapped to the forwarding ASIC.

Workaround: Remove the TE tunnels in the core or have the core link on the forwarding ASIC.

- CSCuc25347

Traffic drop is observed on egress direction of L2VPN when cos filtering is configured on EVC.

Conditions: Egress cos filtering with L2VPN drops packets.

Workaround: Attach pseudowire-class with interworking type as ethernet VLAN.

## Open Caveats for Cisco Release 15.2(4)S2

- CSCts82886

DHCP snooping binding is not established on an EVC BD trusted port.

Conditions: When DHCP snooping is enabled on one or more VLANs and EVC BD is configured on a trusted port that is connected towards the SP network/DHCP server, the client does not receive the IP address and DHCP snooping binding is not established.

Workaround: None. Only the switchport can be configured as a trusted port for now.

- CSCtx95340

Policy-map gets accepted at port-level even if the sum of the child bandwidth is more than the parent shaper value.

Conditions: Policy-map on the service instance is added first and then the port-shaper value is added.

Workaround: Design the QoS policy-map so that the parent shaper value is equal to or more than the sum of the child bandwidths.

- CSCty16119  
MAC withdrawal does not occur.  
Conditions: This issue is observed upon shutting the VFI's VLAN on NPE. Failure of the spoke VC works as expected.  
Workaround: Fail only the spoke VC without affecting the VFI and core VCs on NPE1.
- CSCty31982  
The port-channel is in a suspended state, with the peer throwing messages that LACP is not enabled on the remote node.  
Conditions: This issue is observed upon reload.  
Workaround: Remove/add the untagged service instance that has l2peer STP and LACP configured.
- CSCty78883  
When DHCP requests are sent to renew the allocated IP address, and DHCP host tracking is enabled on the switch, the CPU utilization periodically reaches 100%.  
Conditions: DHCP snooping is enabled on one or more VLANs on the Cisco ME 3600X and ME 3800X running IOS 15.2(2)S or a higher version. DHCP snooping host tracking is configured. A DHCP renew request is sent from a DHCP client.  
Workaround: Disable DHCP snooping host track CLI.
- CSCtz11548  
Confirm and Exceed action counters in the show policy-map interface are not getting cleared with scale configurations upon executing the **clear counters** command.  
Conditions: Observed when executing the **clear counters** command.  
Workaround: Remove the policy-map and add it back.
- CSCtz46946  
Traceback message is observed upon creating a TE tunnel with 6PE/6VPE configuration. No functionality impact.  
Conditions: Configure 6PE/6VPE and create a TE tunnel with autoroute announce.  
Workaround: None.
- CSCtz77011  
Multicast traffic may not be forwarded correctly when traffic is received on a layer 2 port-channel.  
Conditions: This issue is observed with a pair of Cisco ME switches with layer 2 port-channel in between, with layer 2 access port on the non DR PIM neighbor.  
Workaround: Create a dummy portchannel1 (poch1) and start using from portchannel2 until portchannel26. Do not use the dummy portchannel1.
- CSCua22991  
Nuclear Header Error Message is observed.  
Conditions: These messages are observed only if more than one OSPF neighbors is established with more than one RoutedPseudowire enabled interface and OSPF flaps.
- CSCua39229  
IPPS configuration is rejected while changing router roles from master to slave or slave to master with IPPS configuration.

Conditions: The configurations input 1pps 0/0 on the master and output 1pps 0/0 on the slave are not deleted when PTP is unconfigured.

Workaround: Unconfigure input 1pps 0/0 or output 1pps 0/0 before unconfiguring PTP.

- CSCub04782

In a 1:1 (one active and one standby) scenario, when the hot standby converges to active, the port-channel does not come down, but the REP is re-converging. The fast-switch over happens in nearly 1 second.

Conditions: This issue is observed in a 1:1(one active and one-standby) scenario, when the hot standby converges to active.

Workaround: None.

- CSCub11348

Broadcast traffic flows over the Standby Spoke VC and then gets punted.

Conditions: The traffic comes over the Core VCs (as they are up) and the flows over the Standby Spoke VC from Hub to Spoke. In the Spoke, the traffic received from the Spoke VC gets punted to the CPU (Software Forwarded).

Workaround: None.

- CSCub24496

On the Loopback interface used for BGP neighbor establishment, deleting the ip pim sparse-mode and adding back ip pim sparse-mode results in traceback messages. Memory leaks are also observed after this.

Conditions: This issue is observed under the following conditions:

- The Cisco ME 3600X is running Cisco IOS Release 15.2(4)S.
- The multicast stream can be received on any type of interface (L2/L3).

Workaround: None.

- CSCub33943

On the Cisco ME 3600X and ME 3800X, running IOS 15.2S or earlier, when EVC BD is configured on more than 1 port and modification of encapsulation and BD are done on the ports, an assert accompanied with traceback message is thrown with decode pointing to L2 Multicast MET.

Conditions: This issue is observed only with the following sequence of steps, even when IGMP snooping is disabled by default:

1. Configure EVC BD on first gigE port.
2. Configure EVC with same BD on second gigE port.
3. Modify EVC encap and BD on first port.
4. Modify EVC encap and change BD on second port to same value as the first port.

Workaround: The above issue does not occur when steps 3 and 4 (above) are reversed; in other words, when EVC BD is modified on the second port followed by the first port. The issue also does not occur for EVC BD configuration on multiple ports with different BD on each port.

- CSCuc15253

The Cisco ME 3800X stops forwarding traffic and crashes.

Conditions: This issue is observed when a QoS policy applied to a EFP on a 10G interface is removed.

Workaround: None.

- CSCuc15918
 

With the ME3600/ME3800 connected back to back with GIG 0/16, the Multicast traffic does not flow.

Conditions: This issue is observed under the following conditions:

  - The Cisco ME 3600X is running Cisco IOS Release 15.2(4)S.
  - The multicast stream can not be received on GIG 0/16 of interface (L2/L3).

Workaround: None.
- CSCuc23542
 

The PXE client network boot is failing when a Cisco ME 3600X running 15.2(4)S is the DHCP relay agent.

The Cisco ME 3600X is changing the option 54 'DHCP Server Identifier' address to its own ip address in the DHCP Offer received from the PXE DHCP server, causing the client to send his PXE boot request (port 4011) to the Cisco ME 3600X instead of to the PXE server.

Workaround: Downgrade the Cisco ME 3600X to the latest 15.1(2)EY release.
- CSCuc36156
 

DWDM SFP+ are supported in Cisco ME 3600X switches, but when inserted, this switch is not recognizing those DWDM in the SNMP ENTITY-MIB.

Conditions: When a DWDM SFP+ is present on the Cisco ME 3600X switch.

Workaround: None.
- CSCuc59765
 

The Cisco ME 3800X and ME 3600X fails to trigger a watchdog crash in certain scenarios.

Conditions: This issue is observed with soaking over a prolonged period of time.

Workaround: None.
- CSCuc90854
 

Table-map marking is not getting removed after deleting the class-default.

Conditions: Packets continue to get marked as per previous table-map config, even when the configuration is deleted.

Workaround: Detach and re-attach the policymap.
- CSCuc93165
 

With scale EVC Xconnect configuration and same policy-map applied on all of the EVCs, deleting and adding a user-defined class-map results in assert messages on the forwarding ASIC.

Conditions: This issue is observed upon adding and deleting the user-defined class-map.

Workaround: Remove the policy-map and make the dynamic modification on the policy-map. Or, there has to be a delay in the removal and addition of the class-map.
- CSCud06908
 

The Cisco ME 3800X and a Cisco 7600 are working as PE devices, and they have multiple core connections between them. If we bounce one of the core interfaces between the Cisco ME 3800X and the Cisco 7600 and the attachment circuit (AC) simultaneously on the Cisco ME 3800X, we see that the VPLS status on the Cisco ME 3800X shows as up but it shows as down on the Cisco 7600.

Conditions: There should be multiple connection between core devices.

Workaround: Bounce the attachment circuit on the Cisco 7600 to resolve the issue.

- CSCud33887  
6VPE packets get punted and policed.  
Conditions: ESP header is enabled.  
Workaround: None.
- CSCud38386  
Traffic forwarding on EFPs fails after removing MAC-security.  
Conditions: When removing MAC-security with the deny option from EFP, traffic fails to be forwarded on that EFP.  
Workaround: Remove and re-add the service instance.
- CSCud38859  
On the Cisco ME 3600X, need support for dot1dBasePortIfIndex OID.  
Conditions: SNMP walk OID dot1dBasePortIfIndex (.1.3.6.1.2.1.17.1.4.1.2) does not work.  
Workaround: None.
- CSCud42372  
A CPU hog, followed by a crash, is observed.  
Conditions: Peer device flap or network instability can cause this issue.  
Workaround: This issue does not occur on a stable network.
- CSCud45445  
Y1731PM is not working in the following situations:
  - If **rewrite ingress tag pop 1 symmetric** is at the core facing interface.
  - On a Q-in-Q configured interface.

Conditions:

The core facing interface is configured as **rewrite ingress tag pop 1 symmetric**, as follows:

```
interface GigabitEthernet0/9
switchport trunk allowed vlan none
switchport mode trunk
service instance 1 ethernet test
encapsulation dot1q 151
rewrite ingress tag pop 1 symmetric
bridge-domain 151
!
end
```

The Q-in-Q interface is configured as follows:

```
interface GigabitEthernet0/1
switchport trunk allowed vlan none
switchport mode trunk
service instance 1 ethernet test
encapsulation dot1q 151 second-dot1q 110
bridge-domain 151
cfm mep domain 17 mpid 555
cos 1
!
```

Workaround: None.

- CSCud45631

With two separate XFPs installed in ports Te0/1 and Te0/2, the optic types reported by the **show interface status**, **show interface TeX/X capabilities**, and the **show interfaces tenGigabitEthernet X/X transceiver properties** commands are not accurate.

Conditions: This issue is observed upon inserting two different types of XFPs in a Cisco ME 3600X running 15.2(4)S1.

Workaround: To verify that XFP is installed, run one of the following commands: **show controllers ethernet-controller tenGigabitEthernet 0/1 phy** or **show inventory**.

## Open Caveats for Cisco Release 15.2(4)S3

- CSCub11348

Broadcast traffic flows over standby spoke VC and then gets punted.

Conditions: The traffic comes over the core VCs as they are up and then flows over the standby spoke VC from hub to spoke. In the spoke, that traffic received from the spoke VC gets punted to the CPU (software forwarded).

Workaround: There is no known workaround.

- CSCuf43673

The following messages are output, and system crash occurs on an ME3600X node:

```
Mar 15 05:01:40.999 JST: %PLATFORM_NCEF-3-ADJ: NULL OCE handle for fib
10.239.145.114/32 Tbl:1
-Traceback= 641BB8z 2C198D4z 2C2BF44z 2C32DB4z 2C2F564z 2C2BCFCz 2C27640z 2C63810z
2C5ECD0z
Mar 15 05:01:42.539 JST: %SYS-2-CHUNKBADROOTCHUNKPTR: Bad root chunk pointer in chunk
header, chunk 0x12B8C3FC data 0x12B81318 root chunk ptr 0x0
-Process= "Check heaps", ipl= 0, pid= 5 -Traceback= 641BB8z 17CA67Cz 17CB1DCz
17F1BFCz 2C63810z 2C5ECD0z
Mar 15 05:01:44.519 JST: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than
(2000)msecs (13/10),process = Check heaps.
-Traceback= 0x2491838z 0x2492390z 0x20BFDECz 0x20C14D0z 0x20BE958z 0x17ED274z
0x17CB860z 0x17CA68Cz 0x17CB1DCz 0x17F1BFCz 0x2C63810z 0x2C5ECD0z
```

Conditions: System crash occurs on an ME3600X node after changing route-map on route-reflector that establishes ME3600X.

ME3600X is route-reflector-client. The route-map setting that you change on route-reflector is output route-map for another route-reflector-client, not for ME3600X.

Workaround: None.

- CSCug33345

ARP resolution gets failed for a vlan after enabling DAI on another VLAN.

Conditions: This issue is seen after enabling DAI on another VLAN.

Workaround: Enable DAI on VLAN of interest.

## Open Caveats for Cisco Release 15.2(4)S4

- CSCub11348

Broadcast traffic flows over the Standby spoke virtual circuit (VC) and then gets punted.

Conditions: This issue occurs when there is traffic over the Core VCs (as they are `up`) and then flows over the Standby spoke VC from Hub to Spoke. In the spoke, the traffic received from the spoke VC gets punted to the CPU.

Workaround: There is no workaround.

- CSCuc90854

Table-map marking is not getting removed after deleting the class-default.

Conditions: Packets continue to get marked as per previous table-map config, even when the configuration is deleted.

Workaround: Detach and re-attach the policymap.

- CSCud43017

The Precision Timing Protocol (PTP) session does not start on removing the registered loopback interface for the master-slave setup.

Conditions: This issue occurs when the loopback interface (that is used in PTP configuration) is deleted and added back after the PTP is configured.

Workaround: First add the loopback interface and then reconfigure the PTP session.

- CSCue17158

Drop rate is not displayed with Ingress policing policy.

Conditions: This issue occurs when an ingress policer with exceed action has drop rate displayed as zero(0).

Workaround: Drop rate can be measured from the conform and exceeded BPS.

- CSCuf30192

Symptom: Multicast traffic stops getting forwarded when a MROUTER (SVI) VLAN is shut. The incoming interface and outgoing interface are on same VLAN.

Conditions: This issue occurs when IGMP snooping has to be enabled, and SVI has to be acting as a MROUTER. When this MROUTER is shut, traffic should still flow, because L2 connectivity is up. But an outage is observed.

Workaround: Enable and disable IGMP snooping.

- CSCuf54949

QoS memory chunk leaks are seen.

Conditions: This issue occurs only on doing clear counters with egress policy-map applied on interface.

Workaround: There is no workaround.

- CSCug07397

Dynamic deletion of the class-map filter does not take effect in policy-map.

Conditions: This issue occurs when deleting the class-map filter operation does not work. Dynamic deletion still classifies and applies the policer actions under the same class.

Workaround: Detach and reattach the policy-map.

- CSCug33146

OSPF/LDP packets are not punted to the CPU despite having IP enabled on the VLAN.

Conditions: VLAN up trigger to multicast is missed. This is a very rare case. This happens in an environment where VLAN up and down is common.



Workaround: Perform a shut/no shut on the VLAN.

- CSCug58425

MAC flaps seen in VPLS hub-spoke model.

Conditions: This issue occurs when the first VC that comes up is a spoke VC.

Workaround: Reconfigure Layer 2 VFI or flap the VLAN interface.

- CSCui45810

Blocking (BLK) or Alternate (Altn) state trunk link starts forwarding traffic causing a loop for EIGRP hellos.

Conditions: This issue occurs while adding or deleting a VLAN from an allowed VLAN list on a trunk link that is in BLK state.

Workaround: Perform a shut/no shut of the trunk links.

## Resolved Caveats for Cisco Release 15.2(4)S1

- CSCub62897

SVI link up delay issue on flexlink with VLB and Preemption.

SVI is not coming up for a long time, even though there are active ports in that VLAN. This issue occurs with flexlink + preemption + VLAN load balance configuration.

Conditions: Flexlink with preemption and VLAN load balance.

Workaround: None.

- CSCub93654

On the Cisco ME 3600X or Cisco ME 3800X, an ACL applied on an SVI affects I2 switched traffic.

Conditions: None.

Workaround: Explicitly add an ACL entry to allow intra-VLAN traffic.

- CSCuc08306

Cisco ME 3600X QoS: Cos-inner value has to be preserved in the case of POP2.

In an EVC POP1 - POP2 scenario, the egress **set cos** command previously wrote cos of both outer VLAN and VLAN-inner. Now the egress **set cos** command writes cos of only the outer VLAN.

Workaround: None.

- CSCuc25940

The Cisco ME 3800X crashes during an interface flap.

CPU hog errors may also be seen at the time of the crash (such as SYS-3-CPUHOG). The task is running for (186028) msec, more than (2000) msec (1/0), process = Non-Qos Events Process.

Conditions: IGMP and SVI are configured.

Workaround: None.

## Resolved Caveats for Cisco Release 15.2(4)S2

- CSCtz58391

Cisco ME 3600X: Ingress QoS TCAMs are not cleared after certain dynamic changes.

Conditions: Upon removing the encapsulation from the service instance and then deleting the service instance, QoS TCAMs are not cleared.

Workaround: Instead of deleting the encapsulation first, delete the service instance.

- CSCub22049

Native mcast traffic is not forwarded over the forwarding ASIC after a core INTF shut/no shut operation.

After the repetitive trigger on mVPN setup on the router (such as core INTF shut/no shut), one of the native multicast streams of terrain is not flowing as expected.

Workaround: Perform one of the following commands:

```
clear ip mroute <mcast_group>
clear ip route *
```

- CSCub34595

Enabling Dynamic ARP Resolution (DAI) on a VLAN may cause ARP resolution to fail for hosts in other VLANs.

Workaround: Enable DAI for the failing VLAN with IP ARP inspection trust. For example:

```
ip arp inspection vlan 30
int gi 0/10
 ip arp inspection trust
int gi 0/11
 ip arp inspection trust
```

- CSCub98385

CFM over Xconnect remote MEPs are not learned.

Conditions: Have CFM over Xconnect on the Cisco ME 3600X and TE tunnels in the core. Core link is mapped to the forwarding ASIC.

Workaround: Remove the TE tunnels in the core or have the core link on the forwarding ASIC.

- CSCud17700

Upon executing the **sh inv** command when SFP-10G-LR SFP-10G-SR is present in a Cisco ME 3800X or ME 3600X, the description is missing.

Conditions: SFP-10G-LR SFP-10G-SR should be present in 10G ports.

Workaround: None.

- CSCud46291

The Cisco ME 3600X-24CX switch crashes.

Conditions: An exception is observed when an unsupported 3rd party SFP with invalid EEPROM content is inserted and replaced with a Cisco supported SFP when the interface is in an error-disabled state.

Workaround: Use a supported SFP.

## Resolved Caveats for Cisco Release 15.2(4)S3

- CSCtz11548

Confirm and Exceed action counters in the show policy-map interface are not getting cleared with scale configurations upon executing the **clear counters** command.

Conditions: Observed when executing the **clear counters** command.

Workaround: Remove the policy-map and add it back.

- CSCtz60398

Continuous platform asserts failure traceback message with CFM over Xconnect on the box.

Conditions: This issue occurs with CFM over Xconnect with MPLS TE in core. Flap the core facing link.

Workaround: None.

- CSCtz77011

Multicast traffic may not be forwarded correctly when traffic is received on a layer 2 port-channel.

The PIM DR forwards traffic onto the layer 2 port-channel, while the other node only has a \*,G entry. In this situation, the traffic is not forwarded out of the layer 2 port with receivers.

Conditions: This issue is observed in a setup with two Cisco ME 3600X with layer 2 port-channel in between and mVPN. This issue is observed only on port-channel 1.

Workaround: Avoid port-channel 1 by creating a dummy port-channel 1 and start using from port-channel 2 until port-channel 126.

- CSCua39229

1PPS configuration is rejected while changing router roles from master to slave or slave to master with 1PPS configuration.

Conditions: The configurations input 1pps 0/0 on the master and output 1pps 0/0 on the slave are not deleted when PTP is unconfigured.

Workaround: Unconfigure input 1pps 0/0 or output 1pps 0/0 before unconfiguring PTP.

- CSCuc15253

The Cisco ME 3800X stops forwarding traffic and crashes.

Conditions: This issue is observed when a QoS policy applied to a EFP on a 10G interface is removed.

Workaround: None.

- CSCuc36156

DWDM SFP+ are supported in Cisco ME 3600X switches, but when inserted, this switch is not recognizing those DWDM in the SNMP ENTITY-MIB.

Conditions: When a DWDM SFP+ is present on the Cisco ME 3600X switch.

Workaround: None.

- CSCuc38395

ME3600X: Unexpected deferred is counted in certain conditions.

Conditions: Unexpected deferred is counted on egress interface in MPLS network, although the duplex setting is full.

Workaround: None.

- CSCuc59765

The Cisco ME 3800X and ME 3600X fails to trigger a watchdog crash in certain scenarios.

Conditions: This issue is observed with soaking over a prolonged period of time.

Workaround: None.

- CSCud19010

The following DWDM SFPs do not work on a GE or 10GE port on ME3600:

- DWDM-SFP-3346
- DWDM-SFP-3739
- DWDM-SFP-4134
- DWDM-SFP-4532
- DWDM-SFP-4931
- DWDM-SFP-5332
- DWDM-SFP-5736

The same SFP works on a ME3400. When insert one of the DWDM SFPs above into a GE or 10GE port on ME3600 or ME3800, the switch logs the following error messages:

```
%PHY-4-SFP_NOT_SUPPORTED: The SFP in Gi0/3 is not supported
%PM-4-ERR_DISABLE: gbic-invalid error detected on Gi0/3, putting Gi0/3 in err-disable
state
```

Conditions: This issue applies to ME3600 and ME3800. The problem is verified in 15.2(4)S1.

Workaround: None.

- CSCud22527

When MAC security is configured on a EFP port, traffic received on this EFP and designated to one MAC address learned on the same EFP is bounced back on the EFP.

Conditions: The traffic is not bounced back during one of the following conditions:

- MAC security is removed.

or

- Split-horizon group is configured on the EFP.

or

- EFP is replaced by a legacy L2 trunk.

Workaround: None.

- CSCud68830

The Cisco ME3600/ME3800 causes traffic loss or intermittent end-to-end ping drops.

Conditions: This symptom is observed when excess of ICMP redirects in network comprising of Cisco ME3600/ME3800.

Workaround: None.

- CSCud90752

The MAC flaps in the network happen on the reload of the device.

Conditions: The MAC flaps occur because multicast BPDUs are being sent back into the VPLS core after they reach the destination. This behavior causes MAC flaps on every device that is on the path through which the BPDU traverses.

Workaround: Apply split horizon at the bridge-domain where the MAC flaps happen.

- CSCud92714

Cannot configure max mtu when channel-port deleted and re-added.

Conditions: When the port-channel is deleted and created again, the max MTU cannot be set up.

- Workaround: Reload the device.
- CSCue01649  
CPU errors are seen with (\*, G/M) entries on ACL.  
Conditions: This symptom is seen on ME3600CX boxes operating in Mode 3 or Mode 4.  
Workaround: Operate the ME3600CX boxes in Mode 2.
  - CSCue02251  
During archive download to upgrade a software version, an old image present in the board does not get deleted or displayed.  
Conditions: This symptom occurs during an archive download.  
Workaround: None.
  - CSCue07657  
CFM is working under EVC BD configuration on CE6 and CE7 uplink port. But ip sla is unstable in single link scenario. The network is enhanced to a dual link path connection with ME3600. We need to enable Flex-link feature at CE6 and CE7 (ME3600) for dual link scenario and found that the CFM cannot formed by peer.  
Since Flex-link is not supported on EFP interface, uplink port was changed to a switchport setting at CE6 and CE7. The CFM remote maintenance-points were not formed on the CE (ME3600) at the peering end.  
Conditions: On IOS 15.2(4)S, with flexlink configured on uplink ports, CFM remote MEPs do not come up.  
Workaround: Manual switchover of flexlink ports until platform forwarding vlist is not empty. This causes CC packets to be sent correctly and remote MEPs come up.
  - CSCue15539  
L3 traffic failure.  
Conditions: This issue occurs when configuring 4n+1th EFP in a bridge-domain where n=1,2, an so forth.  
Workaround: Clear MAC-address table.
  - CSCue30590  
Packet loss are seen over pseudowire and high CPU.  
Conditions: This symptom is observed when IPv6 site-local multicast MAC traffic is sent over SVI EoMPLS. The traffic is looped between the PE of the EoMPLS.  
Workaround: None.
  - CSCue61393  
Ingress classification based on numbered IP ACL does not work correctly.  
Conditions: If an ingress QoS policy contains match based on numbered ACL, classification does not work, and the actions do not take effect.  
Workaround: Use a named ACL instead of numbered ACL for the match.
  - CSCue89385  
ME3600 Traffic from routed VPLS not triggering ARP.

Conditions: This symptom is observed in a routed VPLS network that has multiple CE routers connected to the PE router. The issue occurs when a local CE router is connected to the PE router via an EVC and when a ping is sent from a local CE router to the remote CE router.

Workaround: Ping the first interface VLAN of the EVC to resolve the ARP.

- CSCuf06660

ACL configured on switchport denies all VRF forwarded traffic in hardware.

Conditions: This issue occurs with VRF forwarded traffic.

Workaround: None.

- CSCuf16072

When trying to upload an image by using **archive upload-sw**, however, the temp dir "ramfs:update" was not created, and the upload failed.

Conditions: None.

Workaround: Use copy flash: tftp: instead.

- CSCuf25555

Policy-based routing stops working after the router reloads.

Conditions: This symptom occurs when multiple next-hops configured on the same route map are reachable through the same interface.

Workaround: Remove and reconfigure the route-map.

## Resolved Caveats for Cisco Release 15.2(4)S4

- CSCuc49773

Observing CPU hog at IP RIB Update after multiple flaps of IGP and MPLS TE tunnels.

Conditions: This issue occurs when multiple MPLS enabled interface flaps resulting in IP RIB update crash.

Workaround: There is no workaround.

- CSCud45100

The Cisco ME3600X/ME3800X switch does not respond due to crash.

Conditions: This issue occurs when having CFM over xconnect with PC in the core and run Y.1731 DMM on it.

Workaround: There is no workaround.

- CSCud94899

Unexpected huge counter values are observed on gig 0/1 interface and on the port-channel soon after creating any port-channel.

Conditions: This issue occurs when creating a port-channel using gig 0/1.

Workaround: There is no workaround.

- CSCud94967

OSPF on R-PW is bound at exstart/exchange state.

Conditions: The issue occurs when there is CFM configuration on the device; OSPF on R-PW does not get to the full state.

- Workaround: Remove "ethernet cfm global" configuration to bring up OSPF on R-PW.
- CSCue52744  
The VRF dual stack is not working.  
Conditions: This issue occurs when there are 15 VRFs with dual stack and 15 VRFs for IPv4 only.  
Workaround: Maintain all VRFs with dual stack.
  - CSCue58933  
The Cisco ME3600x switch stops responding.  
Conditions: This issue occurs when xconnect interface flaps. This issue is specific to port based EoMPLS.  
Workaround: You may upgrade the software version.
  - CSCue92754  
Console messages display status of internal ports.  
Conditions: This issue occurs when reloading the device.  
Workaround: There is no workaround.
  - CSCue94397  
Trust port configuration is invalid on DHCP snooping over EVC. The DHCP discover request cannot be snooped correctly and will be dropped on EVC in an L2 flat environment.  
Conditions: This issue occurs when configuring a new interface regarding BD of trust port, or when reloading after saving the configuration.  
Workaround: There is no workaround.
  - CSCue97277  
VRF ping does not work after deleting and recreating the VRF.  
Conditions: This issue occurs when VRF is deleted and added back multiple times.  
Workaround: There is no workaround.
  - CSCug22139  
When an ACL with the range command is used for QoS, traceback messages are observed.  
Conditions: This issue is observed when the policy-map is applied to the interface. The specified range is 1024 to 65535.  
Workaround: Apply the same ACL, but modify the range to 1024 to 65534.
  - CSCug29132  
Measurements are not done when the active flex link port is down and the standby takes over as the active port on the Cisco ME3600X or Cisco ME3800X switch.  
Conditions: This issue occurs on the Cisco ME3600X or Cisco ME3800X switch running Cisco IOS Release 15.2(4)S1, 15.3(1)S, or 15.3(2)S with:
    - UP MEP is configured
    - Flex link is configured on uplink ports
    - Y1731 SLM is active on the flex link
 Workaround: There is no workaround.
  - CSCug33345

Address Resolution Protocol (ARP) resolution fails when Dynamic ARP Inspection (DAI) is enabled.

Conditions: This issue occurs after enabling the DAI on another VLAN.

Workaround: Enable DAI on the relevant VLAN.

- CSCug33386

Frame loss is observed when configuring an existing class-map to a new service instance. The frame loss is observed on the existing service instance.

Conditions: This issue is observed when the class-map has the same value as the SET value (such as SET DSCP and SET QOS group).

Workaround: There is no workaround.

- CSCug33828

After the reload of Cisco ME3600X switch, a part of the configuration disappears. As a result, a portion of the network does not work until those commands are added back to the configuration.

Conditions: This issue occurs after a reload.

Workaround: There is no workaround.

- CSCug39331

When changing a QoS policy for classification, such as altering a class-map or changing an associated ACL, while the policy is attached to an interface, the classification stops working and remarks traffic in a strange way.

Conditions: This issue is observed when changes are made to the match statement on the class-map or in the access-list.

Workaround: Remove the policy from the interface and reattach it.

- CSCug50156

Traceback messages are observed when the interface is removed and added back quickly.

Conditions: This issue occurs when the interface is removed or configuration is replaced such that a port is removed and added back quickly.

Workaround: There is no workaround.

- CSCug73982

Static MAC address configured on the same VLAN disappears after reload.

Conditions: This issue occurs when the static MAC address is configured on the same VLAN.

Workaround: There is no workaround.

- CSCug74906

Wrong threshold warning messages are displayed for several SFPs.

Conditions: This issue occurs only for the BX\_U and the BX\_D SFPs.

Workaround: There is no workaround.

- CSCug88920

The configuration disappears after a switch reload when the speed is configured with a value equal to 1000 and duplex is configured as "full".

Conditions: This issue occurs after a switch reload.

Workaround: Perform a reconfiguration.



- CSCug99066  
IGMP Snooping is not functional on adding new interface.  
Conditions: This issue occurs when IGMP Snooping is enabled, and when TCN is disabled.  
Workaround: There is no workaround.
- CSCuh82969  
“Receive Power Threshold(++,+,-,--)” is not displayed by the command show interface transceiver.  
Conditions: This issue occurs on the Cisco ME-3800X-24FS-M device running 15.3(2)S1.  
Workaround: There is no workaround.
- CSCui03829  
On the Cisco ME3600X/3800X switch, RIP packets are not punted to CPU from routing TCAM. This is because the CPU is not attached to the TCAM. This results in all the control plane using Multicast RR entry to go down.  
Conditions: Under certain rare conditions, the issue can occur when:
  - a. The last EVC on the Bridge-domain is removed
  - b. The IP address on the VLAN corresponding to this BD is removed
  - c. The VLAN/BD is recreated with the new IP address and a new EVC.
 Workaround: There is no workaround.
- CSCui08752  
Ingress marking does not take in the presence of egress marking with egress policer.  
Conditions: This issue occurs when the egress policy class is hit by the traffic stream should have marking along with policer configured while the ingress policy class hit should have ingress marking.  
Workaround: There is no workaround. If marking, ingress and egress is are primary requirement, then policer can be removed at egress and instead can have policer at the ingress side alone.

## Resolved Caveats for Cisco Release 15.2(4)S6

- CSCuj40499  
Symptom:  
Packets drop during the get pause frame even though flow-control on this interface is disabled.  
Conditions:  
This issue occurs when:
  - a get pause frame is received from the connected device
  - flowcontrol is disabled on the interface
 Workaround:  
There is no workaround.
- CSCtu42387  
Symptoms:  
Gigabit and TenGigabit fiber link reporting threshold violation alarm is observed. The following error message is displayed on the ports:

```
"%SFF8472-3-THRESHOLD_VIOLATION: Gi0/11: Rx power high alarm"
```

**Conditions:**

This issue occurs when the interface shut or no shut.

```
SFF8472-3-THRESHOLD_VIOLATION Gi5/1: Rx power low alarm; Operating value:
-28.5 dBm, Threshold value: -24.0 dBm
```

**Workaround:**

Fixing the fiber signal issue or disconnecting the fiber from the transceiver stops the error messages.

## 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](http://www.cisco.com/en/US/products/ps10965/tsd_products_support_series_home.html)

ME 3600X and ME 3600X-24CXswitch:

[http://www.cisco.com/en/US/products/ps10956/tsd\\_products\\_support\\_series\\_home.html](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 ME 3600X-24CX Switch Hardware Installation Guide*
- *Cisco ME 3600X-24CX Switch Getting Started Guide*
- *Installation Notes for the Cisco ME 3600X-24CX Switch Power-Supply and Fan Modules*
- *Regulatory Compliance and Safety Information for the Cisco ME 3600X-24CX Switch*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco 10-Gigabit XFP Transceiver Modules Install Note*
- *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](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*
- *10-Gigabit Ethernet Transceiver 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2011—2014 Cisco Systems, Inc. All rights reserved.

