



Release Notes for the Cisco ME 3800X, ME 3600X and ME 3600X-24CX Switches, Cisco IOS Release 15.4(1)S and Later Releases

December 1, 2014

May 24, 2016

This release note includes important information about Cisco IOS Release 15.4(1)S that run on the Cisco ME 3800X, ME 3600X and ME 3600X-24CX switches.

This release note also includes limitations, restrictions, and caveats that apply to the release.

You can verify the release notes in the following ways:

- 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 9.
- 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 9.

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://software.cisco.com/download/navigator.html>

Contents

- “[Hardware Support](#)” section on page 2
- “[Software Licenses and Features](#)” section on page 4
- “[Upgrading the Switch Software](#)” section on page 8
- “[Installation Notes](#)” section on page 12
- “[New Software Features](#)” section on page 12



- [“Important Notes” section on page 14](#)
- [“Open Caveats” section on page 14](#)
- [“Resolved Caveats” section on page 20](#)
- [“Related Documentation” section on page 34](#)
- [“Obtaining Documentation and Submitting a Service Request” section on page 35](#)

Hardware Support

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>IO mode 1</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>IO mode 2</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> <p>IO mode 3</p> <p>16 GigabitEthernet SFP downlink ports and 3 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-10G-SR, SFP-10G-LR, SFP-10G-ER, SFP-10G-ZR, SFP-10G-LRM, SFP-H10GB-CUxM, 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

Table 1 Supported Hardware (Continued)

Device	Description
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-SX-MMD, GLC-LH-SMD, GLC-ZX-SM, GLC-EX-SMD, GLC-T, GLC-BX-U (CPN 10-2094-02), GLC-BX-D (CPN 10-2093-02), GLC-BX-U, GLC-BX-D, SFP-GE-L, SFP-GE-S, SFP-GE-T, CAB-SFP-50CM, CWDM-SFP-1470, CWDM-SFP-1490, CWDM-SFP-1510, CWDM-SFP-1530, CWDM-SFP-1550, CWDM-SFP-1570, CWDM-SFP-1590, CWDM-SFP-1610, DWDM-SFP-6061, DWDM-SFP-5979, DWDM-SFP-5898, DWDM-SFP-5817, DWDM-SFP-5736, DWDM-SFP-5655, DWDM-SFP-5575, DWDM-SFP-5413, DWDM-SFP-5494, DWDM-SFP-5332, DWDM-SFP-5252, DWDM-SFP-5172, DWDM-SFP-5092, DWDM-SFP-5012, DWDM-SFP-4931, DWDM-SFP-4851, DWDM-SFP-4772, DWDM-SFP-4692, DWDM-SFP-4612, DWDM-SFP-4532, DWDM-SFP-4453, DWDM-SFP-4373, DWDM-SFP-4294, DWDM-SFP-4214, DWDM-SFP-4134, DWDM-SFP-4056, DWDM-SFP-3977, DWDM-SFP-3898, DWDM-SFP-3819, DWDM-SFP-3739, DWDM-SFP-3661, DWDM-SFP-3582, DWDM-SFP-3504, DWDM-SFP-3425, DWDM-SFP-3346, DWDM-SFP-3268, DWDM-SFP-3190, DWDM-SFP-3112, DWDM-SFP-3033, DWDM-SFP-6141
SFP modules supported on the Cisco ME-3600X-24CX	SFP-GE-L, SFP-GE-S, SFP-GE-Z, GLC-LH-SM, GLC-SX-MM, GLC-SX-MMD, GLC-LH-SMD, GLC-T, SFP-GE-T, GLC-FE-100FX-RGD, GLC-FE-100LX-RGD, GLC-LX-SM-RGD, GLC-SX-MM-RGD, GLC-ZX-SM, GLC-ZX-SM-RGD, GLC-BX-U (CPN 10-2094-02), GLC-BX-D (CPN 10-2093-02), and GLC-EX-SMD, GLC-FE-100FX, GLC-FE-100EX, GLC-FE-100ZX, GLC-FE-100LX, GLC-FE-100BX-U, GLC-FE-100BX-D, CWDM-SFP-1470, CWDM-SFP-1490, CWDM-SFP-1510, CWDM-SFP-1530, CWDM-SFP-1550, CWDM-SFP-1570, CWDM-SFP-1590, CWDM-SFP-1610, DWDM-SFP-6061, DWDM-SFP-5979, DWDM-SFP-5898, DWDM-SFP-5817, DWDM-SFP-5736, DWDM-SFP-5655, DWDM-SFP-5575, DWDM-SFP-5413, DWDM-SFP-5494, DWDM-SFP-5332, DWDM-SFP-5252, DWDM-SFP-5172, DWDM-SFP-5092, DWDM-SFP-5012, DWDM-SFP-4931, DWDM-SFP-4851, DWDM-SFP-4772, DWDM-SFP-4692, DWDM-SFP-4612, DWDM-SFP-4532, DWDM-SFP-4453, DWDM-SFP-4373, DWDM-SFP-4294, DWDM-SFP-4214, DWDM-SFP-4134, DWDM-SFP-4056, DWDM-SFP-3977, DWDM-SFP-3898, DWDM-SFP-3819, DWDM-SFP-3739, DWDM-SFP-3661, DWDM-SFP-3582, DWDM-SFP-3504, DWDM-SFP-3425, DWDM-SFP-3346, DWDM-SFP-3268, DWDM-SFP-3190, DWDM-SFP-3112, DWDM-SFP-3033, DWDM-SFP-6141
XFP modules supported on the Cisco ME-3600X-24CX	XFP-10G-MM-SR, XFP10GLR192SR-RGD, XFP10GER192IR-RGD, XFP-10GER-192IR+, XFP-10GER-192LR, XFP-10GER-192LR+, XFP10GZR192LR-RGD, XFP10GLR-192SR-L, XFP10GER-192IR-L, XFP-10GZR-OC192LR, 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 6](#).

The ME3600X-24CX supports the above licenses including the following:

- 10G license
- 1588BC license
- T1/E1 counted license
- OC3 per port license

The ME 3800X supports these licenses and 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 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 7](#).

To install a software image, see the “[Upgrading the Switch Software](#)” section on [page 8](#) 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/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:

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



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

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

Enabling evaluation license on an ME 3600X:

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



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

```
Switch(conf)# exit
Switch# write memory
Switch# 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 will be unusable after the next reload.

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

Table 2 *ME 3600X Supported Features per License*

Metro IP Access (Universal Image)	Advanced Metro IP Access license
<ul style="list-style-type: none"> • Basic Layer 2 features (including 802.1Q) • Ethernet Virtual Circuits (EVCs) • IPv4 routing—RIP, OSPF, 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 with Ethernet Synchronization Messaging Channel (ESMC) • Multi VRF-CE (VRF-Lite) with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP) • Switch Database Management (SDM) templates • Quality of Service (QoS) 	<ul style="list-style-type: none"> • 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 • Virtual Private Lan Service (VPLS)

Table 3 *ME 3600X and ME 3600X-24CX License Scaling and Template*

Supported feature	Metro IP Access		Advanced Metro IP Access		
	Default	IPv4	Default	IPv4	Application template ¹
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	6 K	3 K	4 K
Layer 2 Multicast groups	1 K	1 K	1 K	1 K	1 K
Layer 3 Multicast groups	1 K	1 K	1 K	1 K	1 K
Bridge domains	4 K	4 K	4 K	4 K	4 K
Maximum Pseudowire (EoMPLS or VPLS)	—	—	512	512	512
MPLS VPN	—	—	128	128	128
VRF Lite	128	128	128	128	128
VPLS Instances	0	—	26	26	26
ACL entries	2 K	2 K	2 K	2 K	IPv4: 2 K IPv6: 1 K
Queues	4 K	4 K	4 K	4 K	4 K
Queues per ASIC	2 K	2 K	2 K	2 K	2 K
IPv4 QoS classification	4 K	4 K	4 K	4 K	1 K
Policers	2 K	2 K	2 K	2 K	2 K
EFP	3990	3990	3990	3990	3990
EFPs per Port	3990	3990	3990	3990	3990
STP Instances	128	128	128	128	128
Etherchannel Groups	26	26	26	26	26
Interfaces per Etherchannel Groups	8	8	8	8	8
HSRP/VRRP	128	128	128	128	128
FRR/TE Headend	—	—	512	512	512
FRR/TE Midpoints	—	—	5 K	5 K	5 K
BFD Sessions @ 50 msec	50	50	50	50	50
Number of SVI for Layer 3	128	128	128	128	128
PBR Entries	—	—	—	—	250
BGP Session	100	100	100	100	100
mVPN-MDT	—	—	—	—	250

1. Application Template is applied to both ME3600x -24TS/FS and ME3600x-24CX to enable mVPN, PRB, IGMP-Snooping, IPv6, and IPv6-ACL.

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"> 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 with Ethernet Synchronization Messaging Channel (ESMC) 	<ul style="list-style-type: none"> All features in the Metro Ethernet Services image IPv4 routing—RIP, OSPF, 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) 	<ul style="list-style-type: none"> All features in the Metro IP Services license MPLS MPLS traffic engineering and Fast Reroute MPLS OAM MPLS VPN EoMPLS Pseudowire redundancy Virtual Private Network (VPLS)

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			
	Default	Default	Default	Default	Default	Default	VPNv4	VPNv4+ IPV6	Video Template
MAC table addresses	64 K	128 K	32 K	64 K	128 K	256 K	256 K	256 K	256 K
IPv4 routes	1 K	1 K	42 K	80 K	24 K	32 K	80 K	80 K	80 K
Layer 3 Multicast Groups	0	0	2 K	4 K	2 K	4 K	8 K	2 K	10 K
IPv6 routes	0.5 K	0.5 K	21 K	40 K	12 K	16 K	8 K	40 K	8 K
Layer 2 Multicast Groups	2 K	4 K	2 K	2 K	2 K	4 K	4 K	2 K	10 K
Bridge domains	4 K	4 K	2 K	2 K	4 K	8 K	4 K	8 K	4 K
ACL entries	4 K	8 K	4 K	8 K	4 K	16 K	4 K	4 K	4 K
IPv4 QoS classification	16 K	24 K	16 K	24 K	16 K	24 K	12 K	12 K	12 K
EoMPLS PW (Cisco IOS Release 15.1(2)EY and later)	0	0	0	0	4 K	8 K	8 K	8 K	1 K
MPLS VPN	0	0	0	0	2 K	2 K	2 K	2 K	2 K

Table 5 *ME 3800X License Scaling (Continued)*

Supported Feature	Metro Services	Scaled Metro Services	Metro IP Services	Scaled Metro IP Services	Metro Aggregation Services	Scaled Metro Aggregation Services			
	Default	Default	Default	Default	Default	Default	VPNv4	VPNv4+ IPv6	Video Template
VRF Lite	0	0	2 K	2 K	2 K	2 K	2 K	2 K	2 K
VPLS Instances	0	0	0	0	1 K	4 K	4 K	4 K	4 K
Queues	16 K	32 K	16 K	32 K	16 K	32 K	32 K	32 K	32 K
Queues per ASIC	8 K	16 K	8 K	16 K	8 K	16 K	16 K	16 K	16 K
Policers	8 K	16 K	8 K	16 K	8 K	16 K	16 K	16 K	16 K
EFP	3990	15990	3990	3990	3990	15990	3990	3990	3990
Maximum EFPs per Port	3990	3990	3990	3990	3990	3990	3990	3990	3990
STP Instances	128	128	128	128	128	128	128	128	128
Maximum Etherchannel Groups	26	26	26	26	26	26	26	26	26
Interfaces per Etherchannel Group	8	8	8	8	8	8	8	8	8
HSRP/VRRP	256	256	256	256	256	256	256	256	256
FRR/TE Headend	—	—	—	—	1 K	1 K	1 K	1 K	1 K
FRR/TE Midpoints	—	—	—	—	7 K	7 K	7 K	7 K	7 K
Number of SVI for Layer 3	1 K	4 K	1 K	4 K	1 K	4 K	4 K	4 K	4 K
PBR Entries	—	2 K	—	2 K	—	2 K	2 K	2 K	2 K
BGP Session	100	100	100	100	100	100	100	100	100
mVPN-MDT	—	1 K	—	1 K	1 K	1 K	1 K	1 K	1 K

Upgrading the Switch Software

- [“Finding the Software Version and Feature Set” section on page 9](#)
- [“Deciding Which Files to Use” section on page 9](#)
- [“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 6 Cisco IOS Software Image Files

Filename	Description
me380x-universal-tar.154-1.S2.tar	Cisco ME 3800X universal image.
me380x-universalk9-tar.154-1.S2.tar	Cisco ME 3800X universal cryptographic image. This image has the Metro Ethernet features plus Kerberos and SSH.
me360x-universal-tar.154-1.S2.tar	Cisco ME 3600X universal images.
me360x-universalk9-tar.154-1.S2.tar	Cisco ME 3600X universal cryptographic image. This image has the Metro IP access features plus Kerberos and SSH.
me360x_t-universal-tar.154-1.S2.tar	Cisco ME 3600X-24CX universal image.
me360x_t-universalk9-tar.154-1.S2.tar	Cisco ME 3600X-24CX universal cryptographic image. This image has the Metro Ethernet features plus Kerberos and SSH.

Installing Software Images and Licenses

The Cisco ME 3800X, ME 3600X and ME 3600X-24CX switches are 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

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/docs/ios/fundamentals/command/reference/cf_book.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 9](#) 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://software.cisco.com/download/navigator.html>

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 graphic image, you must also accept the terms and conditions of using crypto graphic 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 192.0.2.1 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://192.0.2.1/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 the 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.153-2.S/me380x-universal-mz.153-2.S.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 provide information on new software features:

- [Cisco IOS Release 15.4\(1\)S](#), page 12
- [Important Notes](#), page 14

Cisco IOS Release 15.4(1)S

The following new software features are introduced in the Cisco IOS Release 15.4(1)S:

- DS3 Framing on OC3 Ports—This feature supports the configuration of DS3 framing on OC3 ports on the Cisco ME3600X-24CX switch.

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/cha/assis/configuration/guide/OC3_Ifc_Module.html

- IP SLA—Service Performance Testing Infrastructure- Starting with Cisco IOS Release 15.4(1)S, the following features are supported on the Cisco ME 3600-24CX switch:
 - Color-aware traffic generation on layer 2 targets
 - Color-aware two-way and passive measurement for layer 2 targets
 - IP traffic generation on layer 3 targets
 - Color-blind and color-aware passive measurement on layer 3 Targets.
 - Color Aware IP flow Generation: differentiated services code point (DSCP) based
 - Color Aware IP flow measurement: DSCP based
 - IMIX Traffic Generation type (combination of 64, 512, and 1518 byte packets)

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/cha/assis/configuration/guide/swy1564.html

- MPLS TE - Bundled Interface—Starting with Cisco IOS Release 15.4(1)S, the MPLS Traffic engineering (TE) Bundled Interface Support feature enables Multiprotocol Label Switching (MPLS) traffic engineering tunnels over the bundled interfaces EtherChannel on the Cisco ME3800, Cisco ME3600 series switches.

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/configuration/guide/swmpls_te_bundled_interface.html

- PTP Redundancy—Starting with Cisco IOS Release 15.4(1)S, you can configure the Slave Clock mode and the Boundary Clock mode in PTP Redundancy.

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/chassis/configuration/guide/swclocking.html

- Remote LFA FRR for TDM on ME 3600X-24CX-M Switch—When a link or a switch fails, distributed routing algorithms compute new routes that take into account the failure. The Loop-Free Alternate (LFA) Fast Reroute (FRR) feature offers an alternative to the MPLS Traffic Engineering Fast Reroute feature to minimize packet loss due to link or node failure. Some topologies (for example the commonly used ring-based topology) require protection that is not afforded by LFA FRR alone. Remote LFA FRR enables you to tunnel a packet around a failed link to a remote loop-free alternate that is more than one hop away. The Cisco ME 3600X-24CX-M switch supports two pseudowire types that utilize CEM transport: Structure-Agnostic TDM over Packet (SAToP) and Circuit Emulation Service over Packet-Switched Network (CESoPSN). Starting with Cisco IOS Release 15.4(1)S, Remote LFA FRR is supported on TDM pseudowires.



Note

The TDM and CEM pseudowires are not supported on the Cisco ME 3600x and ME 3800x switches.

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/configuration/guide/swiprout.html

- VPLS over Remote LFA—When a link or a switch fails, distributed routing algorithms compute new routes that take into account the failure. The Loop-Free Alternate (LFA) Fast Reroute (FRR) feature offers an alternative to the MPLS Traffic Engineering Fast Reroute feature to minimize packet loss due to link or node failure. Some topologies (for example the commonly used ring-based topology) require protection that is not afforded by LFA FRR alone. Remote LFA FRR enables you to tunnel a packet around a failed link to a remote loop-free alternate that is more than one hop away. VPLS (Virtual Private LAN Service) enables enterprises to link together their Ethernet-based LANs from multiple sites through the infrastructure provided by their service provider.

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/configuration/guide/swiprout.html

- Sonet Framing Support on OC3 ports—This feature supports Sonet mode framing on OC3 ports on the Cisco ME3600-24CX switch.

For more information, see

http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.4_1_S/chassis/configuration/guide/OC3_Ifc_Module.html

Important Notes

- FRR failover time is delayed by seconds, when a neighboring router static PoCH is shut down.
- To adjust the channel on a DMDM-XFP-C tunable SFP, proceed as follows:

```
Switch(config)#int te0/1
Switch(config-if)#itu channel 23
Switch(config-if)#end
```



Note

Based on the ITU grid, the channel number can vary.

- During archive download, the following message is displayed:

```
Please wait till you receive the "Image Extraction Done" success message, or any other
message reporting Failure !!!!!
```

If the operation fails, a failure message is displayed citing the cause of failure.

If the operation is successful, no message is displayed.



Note

The archive download files are extracted to a temporary RAM disk. The RAM disk is deleted after the new files are populated in the flash. The "Deleting Ramdisk" informational message is displayed during this RAM filesystem format operation. If the RAM FS is not formatted successfully, the error message "Filesystem "*" not formatted" is also displayed along with this informational message.

Open Caveats

The following sections provide information about open caveats:

- [Open Caveats in Cisco Release 15.4\(1\)S3, page 14](#)
- [Open Caveats in Cisco Release 15.4\(1\)S2, page 14](#)
- [Open Caveats in Cisco Release 15.4\(1\)S1, page 16](#)
- [Open Caveats in Cisco Release 15.4\(1\)S, page 19](#)

Open Caveats in Cisco Release 15.4(1)S3

- CSCui64565—EFP needs to be reconfigured when VPLS is replaced with EoMPLS
- CSCun75614—EVC configured in a bridge-group does not show local mac-addresses
- CSCup98778—MAC flaps in VPLS setup with standby pseudowire AC configuration
- CSCur71282—OSPF packets fail to tunnel over PW

Open Caveats in Cisco Release 15.4(1)S2

- CSCum55294

Symptom: The vlanTrunkPortDynamicState OID is not available when the interface goes up. The switch displays the error 'No Such Instance currently exists at this OID'.

Conditions: This issue occurs under normal conditions. It was first discovered in the Cisco IOS 15.3(3)S release.

Workaround: There is no workaround.

- CSCun75614

Symptoms: The Bridge-domain does not learn the MAC address, but forwards the traffic.

Conditions: This issue occurs when the cross-connect is configured on the switchport. On configuring the switchport for the first time, the configuration is rejected. But, on re-applying, the configuration is accepted.

Workaround: There is no workaround.

- CSCun81754

Symptom: The snmpEngineBoots integer does not increment on the Cisco ME 3600X and ME3800X after the device is reloaded. It rather gets reinitialized.

Conditions: This issue occurs only when the device gets rebooted. However, if we do warm restart the snmpEngineBoots integer increases.

Workaround: There is no workaround.

- CSCun96012

Symptom: The VLAN loadbalancing does not working in REP segment 1.

Conditions: This issue occurs when there are more than one segment on the REP ring. This issue is observing only for Segment 1.

Workaround: Either shut down the other segments or perform a shut followed by no shut on the other alternate port on segment 1.



Note

Wait for the preemption delay time.

- CSCuo34646

Symptom: When the interface transceiver monitoring is disabled, the interface transceiver reappear after a reload.

Conditions: This issue occurs when the interface transceiver monitoring is disabled with the following commands:

```
transceiver type all
no monitoring
```

After a reload, the commands reappear in the configuration.

Workaround: An EEM script can be applied to remove the commands from the configuration at bootup. This EEM script looks for the syslog message indicating the device was reloaded.

```
event manager applet Disable_transceiver_monitoring
event syslog pattern "SYS-5-RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 3.0 cli command "transceiver type all"
action 4.0 cli command "no monitoring"
action 5.0 cli command "end"
action 6.0 syslog msg "EEM disabled transceiver monitoring"
```

If AAA command authorization is enabled, configure 'event manager session cli username <USER_NAME>'. Else, the EEM script fails.

- CSCuo40698
Symptom: CE to CE Ping fails when TE Tunnel is Up on core
Conditions: This issue occurs when ARP does not get resolved.
Workaround: Perform a shut of the tunnel interface and the ping starts working again.
- CSCuo54427
Symptom: The runts and input errors are reported on the interface.
Conditions: This issue occurs on 100FX optics without fiber connected.
Workaround: Connect the fiber.
- CSCuo65201
Symptom: Third party SFP-10G-ZR port is not supported on the Cisco ME3800X switch.
Conditions: This issue occurs when the switch is running the Cisco IOS 15.3(3)S1 release.
Workaround: Use a Cisco SFP+.
- CSCuo85614
Symptom: Occasionally on certain switches, the 10G REP flaps without any apparent trigger in Layer1.
Conditions: This issue occurs when the 10 Gigabit on the Cisco ME3600X is configured for REP.
Workaround: There is no workaround.

Open Caveats in Cisco Release 15.4(1)S1

- CSCud71071
Symptom: Traceback messages are seen on shutting the core facing interface. There is no functionality impact observed in the network.
Conditions: This issue is seen in L2VPN with ECMP. Shutting of one of the ECMP paths lead to the traceback messages on the console.
Workaround: There is no workaround.
- CSCug07397
Symptom: Dynamic deletion of the class-map filter does not take effect in a policy-map.
Conditions: This issue occurs when deleting the class-map filter operation fails. Dynamic deletion still classifies and applies the policer actions under the same class.
Workaround: Detach and reattach the policy-map.
- CSCui16905
Symptom: The Line Remote Defect Indicator (LRDI) alarms are observed on the OC3 controller, even when the controller state is up.
Conditions: This issue occurs under the following condition:
 1. Configure the card type OC3 on the Cisco ME 3600X-24CX switch, say switch A.
 2. Change the framing to SONET.
 3. Save the configuration and then reload.

4. Observe the LRDI alarms on 1/0/1 controller on switch A connected to switch B.

Workaround: Perform a shut/no shut at peer OC3 controller.

- CSCui74304

Symptom: Remote MPLS ping fails in LFA when SVI is one of the core interfaces.

Conditions: This issue occurs when the SVI is one of the core interfaces with IPFRR enabled.

Workaround: FRR over SVI is currently not supported. So, below workarounds can be applied to mitigate this issue.

For OSPF:

```
ip ospf fast-reroute per-prefix protection disable
```

For ISIS:

```
isis fast-reroute protection level-1 disable
```

```
isis fast-reroute protection level-2 disable
```

```
Isis fast-reroute protection disable
```

Use **clear ip ospf/isis process** command after disabling the FRR feature to access respective IGP functionalities.

- CSCui93904

Symptom: Serial interfaces are not responding.

Conditions: This issue occurs when you:

- Delete and recreate the configurations at a physical environment (PE) having a mix of serial ports. That is OC3 serial interface, DS3 CEM and T1 port (serial).
- Run the script.

Workaround: Reload the Cisco ME 3600X-24CX switch.

- CSCuj62741

Symptom: Ping fails for around 35 seconds.

Conditions: This issue occurs due to a change in topology, and when Alternate port becomes Root port in RSTP mode.

Workaround: In the problem state, use the clear arp command to resume the traffic.

- CSCul00120

Symptom: The IP SLA frame transmission does not happen when the IP SLA is configured with a packet profile having outer-vlan, outer-cos and inner-vlan. The Transmission (Tx) count in the statistics goes zero.

Conditions: This issue occurs only when either inner or outer cos is configured in the packet profile.

Workaround: There is no workaround.

- CSCul10443

Symptom: The 10G WAN interface QoS calculations are taking bandwidth of 10Gbps instead of 9.285Gbps.

Conditions: This issue occurs when you configure 10G interface in WAN mode and apply QoS policy.

Workaround: There is no workaround.

- CSCul29028

Symptom: The control protocols flap intermittently when random traffic drops when SPAN is configured. Drops are also seen on interfaces that may or may not be a part of SPAN destination port.

Conditions: This issue occurs when SPAN is configured.

Workaround: Disable the SPAN configuration, especially the egress SPAN.

- CSCul35511

Symptom: Neither the SNMPwalk of EntityPhysical MIB nor the **Show Inventory** command reports the existence of the ME-FANTRAY-XL part.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.

- CSCum01335

Symptom: Packets entering a VRF interface and exiting the MPLS core interface are switched using the global table instead of the VRF table.

Conditions: This issue occurs when packets are punted due to 'egress mpls mtu fail'.

Workaround: Adjust the interface MTU according to the size of the packet, to avoid the punt condition.

- CSCum41874

Symptom: The license boot level tag 'license boot level' appears in **show run** command, and this tag is not removable.

Conditions: This issue occurs when 'license boot level' license boot level is configured and is removed the next time after a reload.

Workaround: There is no workaround.

- CSCum70579

Symptom: The CISCO-EVC-MIB for ME3600X switch is not available with MetroIPAccess license.

Conditions: This issue is observed only with MetroIPAccess license.

Workaround: Upgrade the license to AdvancedMetroIP license.

- CSCum81665

Symptom: Console errors and incremental leaks are observed.

Conditions: This issue occurs when the **clear ip mroute** command is used with PIM-SSM configuration for the core replication.

Workaround: There is no workaround.

- CSCum91147

Symptom: A few transceiver related alarms are not reported in the CLI after running the **show facility-alarm status** command. SNMP traps are not generated either for the same events.

Conditions: This issue occurs when the Cisco ME 3800X switch is running IOS release 15.3(3)S1.

Workaround: There is no workaround.

- CSCum98354

Symptom: Traceback messages are seen with CPU hog messages when applying egress policy-map on L3VPN VRF Interface.

Conditions: This issue occurs when egress policy applied on a physical port which has EFPs under it. Egress policy should have parent policy with match on large number of VLANs.

Workaround: There is no workaround. Use only required number of VLANs in the policy match criteria. Matching on the VLANs that are enabled globally will suffice.

Open Caveats in Cisco Release 15.4(1)S

- CSCui16905

Symptom: The Line Remote Defect Indicator (LRDI) alarms are observed on the OC3 controller, even when the controller state is up.

Conditions: This issue occurs under the following condition:

1. Configure the card type OC3 on the Cisco ME 3600X-24CX switch, say switch A.
2. Change the framing to SONET.
3. Save the configuration and then reload.
4. Observe the LRDI alarms on 1/0/1 controller on switch A connected to switch B.

Workaround: Perform a shut/no shut at peer OC3 controller.

- CSCui19453

Symptom: The local cutover time by shutting down one ECMP path is almost 900ms.

Conditions: This issue occurs when you have two ECMP paths (1 GigE path + 1 Ten GigE path) with higher OSPF cost than ECMP path.

Workaround: There is no workaround.

- CSCui74304

Symptom: Remote MPLS ping fails in LFA when SVI is one of the core interfaces.

Conditions: This issue occurs when the SVI is one of the core interfaces with IPFRR enabled.

Workaround: FRR over SVI is currently not supported. So, below workarounds can be applied to mitigate this issue.

For OSPF:

```
ip ospf fast-reroute per-prefix protection disable
```

For ISIS:

```
isis fast-reroute protection level-1 disable
```

```
isis fast-reroute protection level-2 disable
```

```
isis fast-reroute protection disable
```

Use **clear ip ospf/isis process** command after disabling the FRR feature to access respective IGP functionalities.

- CSCui93904

Symptom: Serial interfaces are not responding.

Conditions: This issue occurs when you:

- Delete and recreate the configurations at a physical environment (PE) having a mix of serial ports. That is OC3 serial interface, DS3 CEM and T1 port (serial).
- Run the script.

Workaround: Reload the Cisco ME 3600X-24CX switch.

- CSCuj32896

Symptom: Serial interfaces are not responding on changing the payload size to 32 at both the physical environments (PEs), even after reverting to the default payload size value (recommend value).

Conditions: This issue occurs when you:

1. Configure the payload size to 32 (this is when the serial interface goes down), and both, the ingress and the egress counters do not increment at both the PEs.
2. Configure the payload size to 1024(default value). The serial interface remains down. Now, only the ingress counters increment at PEs.
3. Serial interfaces at CEs are down. When the transmitter sends a remote alarm, the receiver loses the frame.

Workaround: Reload both the PEs with payload size 1024.

- CSCuj99721

Symptom: Routed Pseudowire (RPW) ping fails from PE to CE, when SplitHorizon Group 2 is configured in access, and if RPW is with Virtual Private LAN Service (VPLS) Virtual Circuit (VC).

Conditions: This issue occurs when the ping fails.

Workaround: Configure SH Group 1.

- CSCul01541

Symptom: QoS Egress policy-map does not get attached on VRF interface. Egress classification does not work.

Conditions: This issue occurs only with a certain sequence. Here is an example:

1. Configure the switchport trunk interface with the allowed VLAN.
2. Set this interface as a default.
3. Configure the same interface as egress VRF interface.
4. Attach the egress policy-map to the interface.

The error 'QoS: out of tcam resources' is displayed.

In some cases, policy-map gets attached but egress classification breaks.

Workaround: There is no workaround.

- CSCul10443

Symptom: The 10G WAN interface QoS calculations are taking bandwidth of 10Gbps instead of 9.285Gbps.

Conditions: This issue occurs when you configure 10G interface in WAN mode and apply QoS policy.

Workaround: There is no workaround.

Resolved Caveats

The following section provides information about resolved caveats:

- [Resolved Caveats in Cisco Release 15.4\(1\)S3, page 21](#)
- [Resolved Caveats in Cisco Release 15.4\(1\)S2, page 21](#)
- [Resolved Caveats in Cisco Release 15.4\(1\)S1, page 23](#)

- [Resolved Caveats in Cisco Release 15.4\(1\)S, page 28](#)

Resolved Caveats in Cisco Release 15.4(1)S3

- CSCum55294—vlanTrunkPortDynamicState OID is not available when interface goes up
- CSCuo31527—OSPF packets are not forwarded
- CSCuo40698—Ping fails with VC OutInterface as TE Tunnel
- CSCuo79578—Crash in the MetroEthernet switch due to memory corruption
- CSCuo85614—REP interface may flap frequently and randomly on the Cisco ME-3600-24CX switch
- CSCuo85634—PTP sideband processor is getting rebooted after every 14day on the Cisco ME-3600-24CX switch
- CSCuo91791—CPUHOG and crash occurs on removing service-policy on the Cisco ME3600 switch
- CSCup12317—Flex link backup is administratively down when VLB config is removed on the Cisco ME3600 switch
- CSCup17593—VLAN interface state is administratively up even when the physical port state is DOWN
- CSCup23126—IPv6 ND fails due to wrong VRF label
- CSCup42207—WANPHY flag j1 transmit shows inconsistent behavior with running-config and startup config.
- CSCup62987—cbQosQueueingCfgBandwidth returns value of zero on the Cisco ME3600 switch
- CSCup98325—QinQ configuration does not process ARP in IOS 15.3(3)S3 on the Cisco ME3800 switch
- CSCuq29134—snmp-server context vlan- configuration are added automatically
- CSCuq96419—Address MCB timeout issue on VSC8574x on the Cisco ME-3600-24CX switch
- CSCuq97183—Port goes into half duplex on the Cisco ME3600 switch
- CSCur02626—Wrong input counters are displayed for service instances if service-policy is attached
- CSCur46230—ARP incomplete on routed Port-channel26

Resolved Caveats in Cisco Release 15.4(1)S2

- CSCuj62741
Symptom: Ping fails for around 35 seconds.
Conditions: This issue occurs due to a change in topology, and when Alternate port becomes Root port in RSTP mode.
Workaround: In the problem state, use the **clear arp** command to resume the traffic.
- CSCul29028
Symptom: The control protocols flap intermittently when random traffic drops when SPAN is configured. Drops are also seen on interfaces that may or may not be a part of SPAN destination port.
Conditions: This issue occurs when SPAN is configured.

Workaround: Disable the SPAN configuration, especially the egress SPAN.

- CSCul35511

Symptom: Neither the SNMPwalk of EntityPhysical MIB nor the Show Inventory command reports the existence of the ME-FANTRAY-XL part.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.

- CSCum08918

Symptom: BFD Fails to Establish Neighbor when running ISIS. After an interface flap or a device reload, a BFD neighbor fails to establish. Protocols registered to BFD like ISIS also fails to establish.

Conditions: This issue only impacts the Cisco ME3600-cx platforms running ISIS with BFD. The issue is seen with the command **show platform ho-fpga tx-buffer-table detail 258**.

Workaround: Flapping the interface (shut/no shut), or removing and reapplying BFD can resolve the issue.

- CSCum11571

Symptom: Priority tagged traffic fails with type-5 VC.

Conditions: This issue occurs when priority tagged (vlan id 0) is sent over vc type-5 with encapsulation default in EVC.

Workaround: Convert the vc type from type-5 to type-4.

- CSCum41874

Symptom: The license boot level tag 'license boot level' appears in **show run** command, and this tag is not removable.

Conditions: This issue occurs when 'license boot level' license boot level is configured and is removed the next time after a reload.

Workaround: There is no workaround.

- CSCum70579

Symptom: The CISCO-EVC-MIB for ME3600X switch is not available with MetroIPAccess license.

Conditions: This issue is observed only with MetroIPAccess license.

Workaround: Upgrade the license to AdvancedMetroIP license.

- CSCum90797

Symptom: Ping loss is seen for significant duration from non-directly connected VRRP device when the MAC address of the end host changes.

Conditions: The issue occurs when the end host device is changed with another device with the same IP address but different MAC address. Due to this issue, the non-directly connected devices are not able to ping to the host.

Workaround: Perform shut and no shut of the SVI on the non-directly connected devices.

- CSCum91147

Symptom: A few transceiver related alarms are not reported in the CLI after running the show facility-alarm status command. SNMP traps are not generated either for the same events.

Conditions: This issue occurs when the Cisco ME 3800X switch is running IOS release 15.3(3)S1.

Workaround: There is no workaround.

- CSCun20476
Symptom: The ECMP max-path can configure 1 to 16 when using MetroIPAccess.
Conditions: This issue occurs when you boot with MetroIPAccess.
Workaround: Use values 1 to 4.
- CSCun35070
Symptom: Targeted LDP session between Customer Edge devices flap every 3 minutes. IGP Interface LDP between CE devices run fine.
Conditions: This issue occurs when MPLS LDP packet is carried over L2VPN cloud with Control word OFF.
Workaround: Configure control word ON in L2VPN cloud.
- CSCun58030
Symptom: The Cisco ME3600X does not display time source information when running PTP.
Conditions: This issue occurs when the ME3600X does not display time source information when running PTP protocol. There is no functional issues noticed with PTP time synchronization. The time source field says "Unknown".
Workaround: There is no workaround.
- CSCun73463
Symptom: System crashes on configuring card type t1/e1 without t1/e1 license on the switch.
Conditions: This issue occurs on configuring card type t1/e1 without t1/e1 license on the switch.
Workaround: Configure card type after having t1/e1 license on the switch.
- CSCun91720
Symptom: The v6 multicast traffic is punted to host queue.
Conditions: This issue occurs on a Layer 2 switch with no multicast configuration.
Workaround: There is no workaround.

Resolved Caveats in Cisco Release 15.4(1)S1

- CSCuc21897
On the Cisco ME3600X-24CX, the Entity MIB is not responding for the T1/E1 controller ports.
Conditions: This issue occurs when you walk entitymib OID for the entPhysicalEntry, no T1/E1 ports details are returned.
Workaround: There is no workaround.
- CSCue72380
Symptom: The policer on the Cisco ME3600x and ME3800x switches do not work after changing the rewrite type dynamically.
Conditions: This issue occurs when the policer has the table-map, and the rewrite type is changed dynamically.
Workaround: Attach and detach the policy.
- CSCue87217
Symptom: The MAC address used by a port-channel is invalid (all zeros).

Conditions: This issue is only seen if a session is created over a port-channel and then the switch is reloaded.

Workaround: Unconfigure and reconfigure the scheduled session instead of restarting it.

- CSCug77067

Symptom: CPU Hog due to BFD process.

Conditions: This issue occurs on flapping BFD enabled port-channel.

Workaround: There is no workaround.

- CSCuh16016

Symptom: QoS-related CPU hog error messages are displayed.

Conditions: This issue occurs when you use the **clear xconnect** command.

Workaround: There is no workaround.

- CSCui11977

Symptom: Memory leak is observed at NQ_PD_POL_ACTION.

Conditions: This incremental leak is observed on dynamic modification of marking with multiple set statements in the class.

Workaround: There is no workaround.

- CSCui23703

Symptom: The following messages are seen on bootup of The Cisco ME3600x and ME3800x switch.

```
*Jul 1 23:25:12.395: NQATM: Ingress aclType should not be used here
```

```
*Jul 1 23:25:13:402: Table type:0, total entries:1024 *Jul 1 23:25:13:402: Table type:1, total entries:1024
```

Conditions: This issue occurs on booting the Cisco ME3600x switch without any configurations.

Workaround: There is no workaround.

- CSCui40318

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

Conditions: This issue occurs while dynamically deleting the class-map filter, and still classifies and applies the policer actions under the same class.

Workaround: Detach and reattach the policy-map.

- CSCui78428

Symptom: An error message is seen upon configuring storm-control.

Conditions: This issue occurs when you configure storm-control with EVCs on the interface.

Workaround: There is no workaround. This is a cosmetic issue and does not affect functionality in anyway.

- CSCuj15984

Symptom: The PTP Slave continues to communicate even after using the **no clock source <ip>** command.

Conditions: This issue occurs under the normal conditions.

Workaround: Unconfigure and reconfigure the PTP feature.

- CSCuj32994
Symptom: The VRF IPv4 ping fails upon removing the IPv6 address.
Conditions: This issue occurs when you remove the IPv6 address under the interface SVI that again is under VRF.
Workaround: There is no workaround.
- CSCuj35358
Symptom: The SPAN sessions are not working on dynamic modification of the session parameters.
Conditions: This issue occurs when you have multiple source ports, which changes SPAN direction.
Workaround: Remove SPAN session and reconfigure.
- CSCuj40499
Symptom: Output packet drop is seen for the pause frames when, receive flow control is enabled on the 1gigabit interfaces.
Conditions: This issue occurs under the following conditions:
 - when you get a pause frame from a connected device
 - when you disable the flowcontrol on the Cisco ME3600x switch interfaceWorkaround: There is no workaround.
- CSCuj53440
Symptom: Traceback messages are seen on switching of SyncE clock reference in the PTP OC master node.
Conditions: This issue occurs when SyncE is configured along with PTP.
Workaround: There is no workaround.
- CSCuj55631
Symptom: QOS invalid policy-map is accepted on EFP.
Conditions: This issue occurs when EFP is not associated with the bridge-domain, or with the cross connect.
Workaround: There is no workaround.
- CSCul01805
Symptom: MAC flaps are seen on a shut service instance after a reboot.

When the Cisco ME600x or ME3800x switch is reloaded with an ethernet service instance in an administratively shutdown state, it reports MAC-flap messages between the administratively down service instance and the another port, if there is a loop with the service instance active.
Conditions: This issue occurs when the MAC-flaps on the shut EFP is seen only at bootup.
Workaround: Perform no shut and shut of the service instance.
- CSCul07367
Symptom: Traffic of Ethertype 0x8847 is not passing through cross connect on the Cisco ME-3600X-24CX-M switch.
Conditions: This issue occurs under normal conditions.
Workaround: There is no workaround.
- CSCul09487

Symptom: A system crash is observed on defaulting an interface which has EFP configurations.

Conditions: This issue occurs when you default an interface which has EFP configurations. It is a timing issue and is not seen everytime an interface is defaulted.

Workaround: There is no workaround.

- CSCul38388

Symptom: In a REP setup, when you have a port in the FAILED state due to NO_NEIGHBOR, and in this state if the other port of the REP segment is brought up and moves to OPEN state, or if the other port is already in OPEN state is shutdown, the FAILED port is gets unblocked in the hardware. This results in a layer 2 loop.

Conditions: This issue is seen only with ports in FAILED state due to no neighbor condition.

Workaround: A shut/no-shut on the FAILED port moves it back to the blocking state.

- CSCul56311

Symptom: Traffic forwarding issue is observed with static MAC address on port-channel. Following are the configuration steps:

1. Configure port-channel
2. Configure static MAC address
3. Save and reboot the system

After the reboot, traffic generated using the static MAC address are not egressing out of the port-channel.

Conditions: This issue occurs after the reboot egress forwarding stops.

Workaround: Reconfigure the static MAC address.

- CSCul63141

Symptom: Layer 2 flow hits the layer 3 ACL entry.

Conditions: This issue occurs when the SVI interface is configured with **no ip unreachable** command.

Workaround: Following are the workarounds:

- Create a specific permit entry for the direction of ping (ICMP traffic) in the ACL.
- Remove **no ip unreachable** command configuration from the SVI.

- CSCul65832

Symptom: Multicast VPN traffic is not received by the receivers.

Conditions: This issue occurs upon starting the multicast traffic and this joins for the VRFs.

Workaround: Increase the MTU size of the core interface in the switch, which is not forwarding the mVPN traffic.

- CSCul73147

Symptom: For CEM MPLS packets imposed with EXP=5 by default, the COS=5 is not set on the MPLS transport VLAN.

Conditions: This issue occurs when the SAToP/CESOP CEM pseudowires are initiated from a PE device and egresses out of the PE device into a layer 2 network, the MPLS transport VLANs COS value is expected to be 5 by default but it is not in this case.

Workaround: There is no workaround. Enter the following command in SD CLI after bootup:

```
sdcli#mydevice pp reg egressqosmactable configure 0 1 cosDeiEgress 1
```

- CSCu182753
Symptom: An invalid 1G MAC port number error message is observed on a flapping 10G interface.
Conditions: This issue occurs under normal conditions.
Workaround: There is no workaround.
- CSCum04999
Symptom: Egress classification is not working on 'switchport trunk' interface with and without allowed VLANs configured.
Conditions: This issue occurs when the egress QoS applied on the interface where 'switchport trunk' interface is configured.
Workaround: There is no workaround.
- CSCum14431
Symptom: MVPN traffic is not received properly by the receivers as the core replication does not work.
Conditions: This issue occurs when a lot of scale is present, or when the data MDT is used with scale for mVPN.
Workaround: Default MDT can be used.
- CSCum14586
Symptom: An invalid QoS configuration gets accepted under EFP without BD or the cross connect.
Conditions: This issue occurs when EFP is configured without BD or the cross connect configuration where validation is missing.
Workaround: There is no workaround.
- CSCum23849
Symptom: The targeted LDP is not working when TE tunnel is through the Cisco ME3600x switch.
Conditions: This issue occurs under the following scenario:
 Scenario: ME3600x-1-----ME3600x-2-----ME3600x-3
This issue occurs when **no mpls ip propagate-ttl forwarded** command is configured on the midpoint router (ME3600x-2).
Workaround: Remove **no mpls ip propagate-ttl forwarded** configuration.
- CSCum57088
Symptom: The Cisco ME 3600X switch does not respond.
Conditions: This issue occurs when a port-channel interface is configured in a bridge-domain where other interfaces are configured for 'l2protocol tunnel lldp' and LLDP packets are received.
Workaround: Remove 'l2protocol tunnel lldp' configuration from the interfaces in the bridge-domain.
- CSCum64231
Symptom: The STP BPDU loss is observed.
Conditions: This issue occurs when BPDUs are tunnelled or forwarded across an EVC cross connect. This issue is not seen with other forms of cross connects, but is specific to Layer 2 Protocol Tunneling (L2PT) forward/tunnel.

Workaround: There is no workaround.

- CSCum81574

Symptom: The ingress PE node with PIM-SSM gets crashed on sending multicast traffic.

Conditions: This issue occurs when the core MDT routes reach around 1k with the video template.

Workaround: There is no workaround.

- CSCun01188

Symptom: The console does not respond.

Conditions: This issue occurs due to the following reasons:

- Large number of global VLANs are active (500 in this case)
- Output policy in trunk port.
- Input policy is configured after output policy attachment.

Workaround: There is no workaround.

Resolved Caveats in Cisco Release 15.4(1)S

- CSCub11348

Symptom: Broadcast traffic flows over the Standby spoke virtual circuit (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, the traffic received from the spoke VC gets punted to the CPU.

Workaround: There is no workaround.

- CSCud41069

Symptom: TCP adjust-mss does not work on the Cisco ME3600X/3800X switch.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.

- CSCue94397

Symptom: 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 layer 2 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.

- CSCuf01706

Symptom: Node crashes when Layer 3 and Layer 2 services are reloaded. This terminates the peer end nodes.

Conditions: This issue occurs when a reload or flap of MPLS interface is enabled at the peer end.

Workaround: There is no workaround.

- CSCuf61563

Symptom: Static MAC address configuration does not drop traffic from the specific MAC.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.

- CSCuf73865

Symptom: Packet corruption is observed with Virtual Private LAN Services (VPLS) VC type 4.

Conditions: This issue occurs when egressing on VPLS VC type 4 from a Cisco ME3600X Switch or a Cisco ME3800X Switch.

Workaround: There is no workaround.

- CSCuf85356

Symptom: The Cisco ME 3600X switch tags packets on the native VLAN of a dot1Q trunk when the packets are routed. Local generated packets goes untagged, and packets that have only been switched through the Cisco ME 3600X goes untagged. But, if the packet enters the Cisco ME 3600X on another VLAN and is routed to the destination VLAN, it gets tagged when leaving on a dot1Q trunk.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.

- CSCuf85418

Symptom: Netflow and BFD configurations on the same interface (Layer 3 port, portchannel, and so on) make BFD unresponsive and BFD stays in the "AdminDown" state.

Conditions: This issue occurs if there is an interface (individual Layer 3 port, port-channel) configured with Netflow and BFD. This issue can occur on the Cisco ME3600X and ME3800X switches.

Workaround: Disable the IP flow ingress command from the interface configured with BFD. Netflow is not supported on the Cisco ME3600X and ME3800X platforms.

- CSCug29132

Symptom: 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.

- CSCug33386

Symptom: 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.

- CSCug36858

Symptom: MET consumption increases on sending traffic through a VPLS configuration. This leads to MET resources being exhausted.

Conditions: This issue occurs while sending traffic through a VPLS configuration.

Workaround: Reload the switch.

- CSCug39331

Symptom: 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.
- CSCug49343

Symptom: Unable to delete pseudowire interface after its creation.

Conditions: This issue occurs when a pseudowire interface defined with only one value is deleted.

Workaround: Define the pseudowire with two numbers. Note the second number as it is not displayed in the running configuration.
- CSCug50399

Symptom: Broadcast traffic sent through span destination port forwards traffic, and other ports of the Cisco ME3800X switch receives it.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.
- CSCug58425

Symptom: 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.
- CSCug73982

Symptom: 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.
- CSCug88920

Symptom: 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

Symptom: IGMP Snooping is not functional up on adding a new interface.

Conditions: This issue occurs when IGMP Snooping is enabled, and TCN is disabled.

Workaround: There is no workaround.
- CSCuh02728

Symptom: ALL IGP protocols generate LSA/LSP for 127.0.0.1/16 and 127.1.0.0/16 network.

Conditions: This issue occurs when the passive interface default is enabled under IGP protocol (OSPF, ISIS, EIGRP, or RIP).

Workaround: Remove the passive interface default from IGP.
- CSCuh09508

Symptom: Traffic is not looped back for EFP with a double tag configured for data plane loopback with cos as the filter criteria for loopback.

Conditions: Traffic to be looped back is having q-in-q tags and different outer cos and inner cos specified. Loopback is configured with cos match criteria.

Workaround: Traffic to be looped back should have both outer and inner cos as same value and this cos value should be used in the data plane loopback configuration.

- CSCuh24470

Symptom: Missing packets and jitterbuffer underrun counters are incrementing on a Cisco ME3600CX node where E1 pseudowire (SATOP) is created between a Cisco ME7600 and the Cisco ME3600CX over the MPLS cloud.

Conditions: This issue occurs when trigger for this issue is to add "mpls ldp explicit null" on PE routers.

Workaround: There is no workaround.

- CSCuh27825

Symptom: High CPU utilization is observed due to an NL3U background process, and this happens once all resources are exhausted.

Conditions: This issue occurs due to many failed adjacencies.

Workaround: Reload the box.

- CSCuh69131

Symptom: A few units show ping loss to an extent of about 2-5%, when the ping was on a 10G port.

Conditions: This issue occurs when there is a sweep ping traffic over the 10G port.

Workaround: There is no workaround.

- CSCuh71966

Symptom: Traffic drops for a few prefixes.

Conditions: This issue occurs when L3VPN with ECMP paths is configured, and when more than 10K prefixes are populated in the routing table.

Workaround: Remove the ECMP paths.

- CSCuh79802

Symptom: Unable to disable the MAC-learning for VLAN on Cisco ME3600X/ME3800X switches.

Conditions: This issue occurs when a VLAN is not part of the EVC or BD.

Workaround: There is no workaround.

- CSCuh80249

Symptom: The Cisco ME3600X crashes if VRF configuration is removed from routed PW VLAN interface.

Conditions: This issue occurs when the routed PW VLAN interface is configured with the secondary IP address.

Workaround: There is no workaround as there is no support for secondary IP address on routed PW VLAN interface.

- CSCuh82969

"Receive Power Threshold(++,+,-,--)" is not displayed by the show interface transceiver command.

Conditions: This issue occurs on the Cisco ME-3800X-24FS-M device running 15.3(2)S1.

Workaround: There is no workaround.

- CSCui03829

Symptom: On the Cisco ME3600X or 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:

- The last EVC on the Bridge-domain is removed
- The IP address on the VLAN corresponding to this BD is removed
- The VLAN/BD is recreated with the new IP address and a new EVC.

Workaround: There is no workaround.

- CSCui04528

Symptom: The BFD and IS-IS flaps on the systems that are subjected to an ARP storm, either deliberate, or intermittent network topology loops.

Conditions: This issue occurs under exceptional cases, where there is a misbehaving CPE, or a broadcast loop that may be created.

Workaround: There is no workaround.

- CSCui10419

Symptom: CC packets are transmitted with BD-Id instead of push tag.

Conditions: This issue occurs when:

- Layer 2 VFI is on access side.
- Core side interface is an MPLS interface.
- EFP encapsulation is set as a default.
- EFP has rewrite push.
- MEP is configured over EFP-BD.

Workaround: There is no workaround.

- CSCui24884

Symptom: The SNMP context cannot be configured on the Cisco ME3600X switch.

Conditions: This issue occurs when the switch is running Cisco IOS 15.2(4) release.

Workaround: There is no workaround.

- CSCui45810

Symptom: 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.

- CSCui47032

Symptom: The DHCP snooping enabled on one VLAN causes failure in DHCP address assignment for DHCP clients on other VLANs.

Conditions: This issue occurs on the Cisco ME3600X/ME3800X switch running IOS 15.3S. The DHCP snooping configuration on a VLAN affects DHCP client address assignment on other VLANs.

Workaround: Disable DHCP snooping feature.

- CSCui73553

Symptom: High CPU utilization with Small form-factor pluggable transceiver SFF-8472.

Conditions: This issue occurs when GLC-LH-SMD is used.

Workaround: Use an SFP without DOM or disable DOM monitor.

- CSCui77188

Symptom: The message "SD read failed!" is seen on IOS bootup.

Conditions: This issue occurs when IOS is booted with SD card (2G 16-3932-01 (C-Temp)) plugged in.

Workaround: Use 2GB: 16-3795-01 (I-Temp) SD card.

- CSCui89743

Symptom: When multiple priority configurations are on the policy-map, an error message is seen that blocks the configuration:

Conditions: This issue occurs when there is a need to set multiple priority on the same policy-map. This is true only for priority levels and not for setting priority.

Workaround: There is no workaround.

- CSCui94366

Symptom: Traceroute ethernet CFM fails on the Cisco ASR9K when the source is the second hop or beyond.

Conditions: This issue occurs under normal conditions.

Workaround: There is no workaround.

- CSCuj73969

Symptom: Observed SVI EoMPLS traffic loss on moving from default to VPNV4-V4 template.

Conditions: This issue occurs when the traffic fails at the disposition.

Workaround: There is no workaround. Changing the template to default works.

- CSCul19148

Symptom: The **.bin** file that is extracted from **.tar** file does not have the right image name. And, when upgrading from 15.3(3)S to 15.3(3)S1 using the **archive download-sw <TAR file>** the router drops to rommon.

Conditions: This issue happens when the **.bin** file is extracted from **.tar** file (and/or) when extracted using the **archive download-sw** command.

Workaround: There is no workaround for the wrong image name. Switch dropping to rommon during the upgrade through archive download-sw command can be avoided by using **archive download-sw** or **leave-old-sw <TAR file>** command.

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 and ME 3600X-24CX 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 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

- *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 and Submitting a Service Request

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

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

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. 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)

© 2014 Cisco Systems, Inc. All rights reserved.

