



# Release Notes for the Cisco ME 3800X, ME 3600X and ME 3600X-24CX Switches, Cisco IOS Release 15.3(1)S and Later Releases

---

April 30, 2013

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 15.3(1)S
- Cisco IOS Release 15.3(1)S1
- Cisco IOS Release 15.3(1)S2

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 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 32.

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 4
- “[Upgrading the Switch Software](#)” section on page 8



---

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

- [“Installation Notes” section on page 12](#)
- [“New Software Features” section on page 12](#)
- [“Important Notes” section on page 15](#)
- [“Open Caveats” section on page 15](#)
- [“Resolved Caveats” section on page 23](#)
- [“Related Documentation” section on page 32](#)
- [“Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page 33](#)

## 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> <p><b>IO mode 3</b></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>

**Table 1** Supported Hardware (continued)

Device	Description
SFP+ modules	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, CAB-SFP-50CM, DWDM-SFP-6061, DWDM-SFP-5979, DWDM-SFP-5898, DWDM-SFP-5817, DWDM-SFP-5655, DWDM-SFP-5575, DWDM-SFP-5413, DWDM-SFP-5494, DWDM-SFP-5252, DWDM-SFP-5172, DWDM-SFP-5092, DWDM-SFP-5012, DWDM-SFP-4851, DWDM-SFP-4772, DWDM-SFP-4692, DWDM-SFP-4612, DWDM-SFP-4453, DWDM-SFP-4373, DWDM-SFP-4294, DWDM-SFP-4214, DWDM-SFP-4056, DWDM-SFP-3977, DWDM-SFP-3898, DWDM-SFP-3819, DWDM-SFP-3661, DWDM-SFP-3582, DWDM-SFP-3504, DWDM-SFP-3425, 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-T, SFP-GE-T, 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, 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-5655, DWDM-SFP-5575, DWDM-SFP-5413, DWDM-SFP-5494, DWDM-SFP-5252, DWDM-SFP-5172, DWDM-SFP-5092, DWDM-SFP-5012, DWDM-SFP-4851, DWDM-SFP-4772, DWDM-SFP-4692, DWDM-SFP-4612, DWDM-SFP-4453, DWDM-SFP-4373, DWDM-SFP-4294, DWDM-SFP-4214, DWDM-SFP-4056, DWDM-SFP-3977, DWDM-SFP-3898, DWDM-SFP-3819, DWDM-SFP-3661, DWDM-SFP-3582, DWDM-SFP-3504, DWDM-SFP-3425, DWDM-SFP-3268, DWDM-SFP-3190, DWDM-SFP-3112, DWDM-SFP-3033, DWDM-SFP-6141

**Table 1 Supported Hardware (continued)**

Device	Description
XFP modules supported on the 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-10GER-192IR+, XFP-10GER-192LR+, 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 6](#).

The ME3600X-24CX supports the above licences 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 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/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:

```
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"> <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 and ME 3600X-24CX License Scaling and Template*

Supported feature	Metro IP Access		Advanced Metro IP Access		
	Default	IPv4	Default	IPv4	Application template <sup>1</sup>
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	4 K	4 K	4 K	4 K	4 K
EFPs per Port	4 K	4 K	4 K	4 K	4 K
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*

<b>Metro Ethernet Services (Universal Image)</b>	<b>Metro IP Services license</b>	<b>Metro Aggregation Services license</b>
<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*

<b>Supported Feature</b>	<b>Metro Services</b>	<b>Scaled Metro Services</b>	<b>Metro IP Services</b>	<b>Scaled Metro IP Services</b>	<b>Metro Aggregation Services</b>	<b>Scaled Metro Aggregation Services</b>			
	<b>Default</b>	<b>Default</b>	<b>Default</b>	<b>Default</b>	<b>Default</b>	<b>Default</b>	<b>VPNv4</b>	<b>VPNv4+ IPV6</b>	<b>Video Template</b>
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	4 K	16 K	4 K	4 K	4 K	16 K	4 K	4 K	4 K
Maximum EFPs per Port	4 K	4 K	4 K	4 K	4 K	4 K	4 K	4 K	4 K
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 10](#)



## 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.153-1.S.tar	Cisco ME 3800X universal image.
me380x-universal-tar.153-1.S1.tar	
me380x-universal-tar.153-1.S2.tar	
me380x-universalk9-tar.153-1.S.tar	Cisco ME 3800X universal cryptographic image. This image has the Metro Ethernet features plus Kerberos and SSH.
me380x-universalk9-tar.153-1.S1.tar	
me380x-universalk9-tar.153-1.S2.tar	
me360x-universal-tar.153-1.S.tar	Cisco ME 3600X universal images.
me360x-universal-tar.153-1.S1.tar	
me360x-universal-tar.153-1.S2.tar	
me360x-universalk9-tar.153-1.S.tar	Cisco ME 3600X universal cryptographic image. This image has the Metro IP access features plus Kerberos and SSH.
me360x-universalk9-tar.153-1.S1.tar	
me360x-universalk9-tar.153-1.S2.tar	
me360x_t-universal-tar.153-1.S.tar	Cisco ME 3600X-24CX-M universal images.
me360x_t-universal-tar.153-1.S1.tar	
me360x_t-universal-tar.153-1.S2.tar	
me360x_t-universalk9-tar.153-1.S.tar	Cisco ME 3600X-24CX-M universal cryptographic image. This image has the Metro IP access features plus Kerberos and SSH.
me360x_t-universalk9-tar.153-1.S1.tar	
me360x_t-universalk9-tar.153-1.S2.tar	

## 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 6 on page 9](#) 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=ahhttp://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 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 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.153-1.S/me380x-universal-mz.153-1.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 the command to install the license:

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

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

```
Switch# config t
Switch(config)# license boot level license_name
```

**Step 4** If you have 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 15.3\(1\)S, page 12](#)
- [Cisco IOS Release 15.3\(1\)S1, page 15](#)
- [Cisco IOS Release 15.3\(1\)S2, page 15](#)

## Cisco IOS Release 15.3(1)S

The following are the new software features introduced in Cisco IOS Release 15.3(1)S.

ITU-T G.8032 Ethernet Ring Protection Switching—This feature implements protection switching mechanisms for Ethernet layer ring topologies. The feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. For details about this feature see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swering\\_prot.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swering_prot.html)

Switch Port Analyzer (SPAN)—This feature allows monitoring of switch traffic on a port or VLAN using a network analyzer or RMON probe. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swSPAN.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swSPAN.html)

IEEE 802.1x - VLAN Assignment—An 802.1x client switch can, once authenticated, receive its VLAN assignment from a RADIUS server. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/sw8021x.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/sw8021x.html)

IEEE 802.1x - Authenticator—IEEE 802.1x is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/sw8021x.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/sw8021x.html)

Cisco ME3600 24CX: HDLC Support on T1/E1 IM—This feature provides HDLC Support on T1/E1 interfaces. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/chassis/configuration/guide/sw\\_T1-E1.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/chassis/configuration/guide/sw_T1-E1.html)

Egress default queue limit improvement and percent bandwidth support—QoS feature to increase QoS Buffer depths and default queue limits on the Cisco ME 3800X/ME 3600X. The feature allows setting queue limits as a percentage of the total buffer pool. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swqos.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swqos.html)

E2E Transparent Clocking—This feature supports E2E Transparent Clocking on the Cisco ME 3600X-24CX. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/chassis/configuration/guide/swclocking.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/chassis/configuration/guide/swclocking.html)

Match Input Interface and VLAN—Support for QoS groups to be configured at multiple level in the egress hierarchy. Prior to this only the PHB level was allowed to be configured with QoS groups. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swqos.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swqos.html)

Enhanced Object Tracking—This feature provides a more complete alternative to the Hot Standby Routing Protocol (HSRP) tracking mechanism, which allows you to track the line-protocol state of an interface. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/sweot.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/sweot.html)

Ethernet Data Plane Loopback—This feature, when enabled, helps to monitor the Data Plane connectivity between two interfaces. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swedpl.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swedpl.html)

LACP 1-1 Redundancy with Fast Switchover—LACP 1-1 redundancy provides an enhancement over the current LACP implementation to support fast failover without link flapping under 1-1 active/hot standby configuration. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swethchl.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swethchl.html)

Max Bundle/LACP Hot Standby—This feature supports LACP Max Bundle and LACP Active Standby. For details about this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swethchl.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swethchl.html)

VPLS over MPLS SVI uplink, EVC Xconnect with MPLS SVI uplink (Switchport or EVC), SVI L3VPN over SVI uplink - MPLS IP on SVI Support—This feature supports the qualification of SVI as an MPLS uplink. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swmpls.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swmpls.html)

EVC Push Rewrite—This feature supports Rewrite Ingress Push 1 on the Cisco ME 3600X/ME 3800X switches. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swevc.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swevc.html)

MPLS-TP MIB—This feature provides support for the MPLS-TP MIB. For details about this feature, see:

[http://www.cisco.com/en/US/docs/ios-xml/ios/mp\\_em\\_and\\_mibs/configuration/15-s/mpls-tp-mib.html](http://www.cisco.com/en/US/docs/ios-xml/ios/mp_em_and_mibs/configuration/15-s/mpls-tp-mib.html)

IPSLA Y1731 SLM Feature Enhancement—This feature provides support for concurrent and on demand ETH-SLM operations on the Cisco ME 3600X/ME 3800X switches. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swy1731pm.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swy1731pm.html)

L2VPN Protocol Based CLI—Adds support for the new protocol based CLI for L2VPN to platforms. This feature unifies the Nexus and IOS CLIs for L2VPN technology. Note that for the time being, we will still honor the old CLI and will follow the standard Cisco/IOS CLI migration model. For details about using this feature, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swl2vpn\\_prot\\_based.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swl2vpn_prot_based.html)

Cisco ME 3600X-24CX I/O Mode 3—Three I/O modes are available on the switch. For more information about the modes, see:

[http://www.cisco.com/en/US/docs/switches/metro/me3600x\\_3800x/software/release/15.3\\_1\\_S/configuration/guide/swsdm.html](http://www.cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/15.3_1_S/configuration/guide/swsdm.html)

Link Path Through—This feature enables a local EoMPLS PE router to detect a failure in the path between the remote PE and CE routers. The local PE router propagates the failure to the local CE router such that it brings down the pseudowire connection and can more quickly reestablish the connection when the remote CE-PE connection is restored. This feature is enabled automatically and does not introduce any new CLI commands.

- This feature is applied only to EoMPLS connections under 'EVC Default' on the Cisco ME 3600X/ME 3800X platform.
- When EoMPLS under EVC default with link path through feature is configured on an interface and if the port is in Remote Link Down state, then if another EVC is configured on the interface, the Link is removed from the Remote Link Down state and does not handle any further Remote Link Down events.
- This feature is not symmetrical if the remote PE does not support EoMPLS remote Ethernet port shutdown and the local PE does support it. This can potentially happen if the remote PE is running an older version of the image or is another platform which does not support this feature while local PE is running an image which supports this feature.

## Cisco IOS Release 15.3(1)S1

This release contains no new features.

## Cisco IOS Release 15.3(1)S2

This release contains no new features.

## Important Notes

- Layer 2 Protocol (L2PT) can forward LinkOAM, ESMC, ELMI, and other reserved MAC addresses in the IEEE range of 0180C2000000-0F.

### Limitations:

- Pause frames that use 0180C2000001 cannot be L2PT forwarded or dropped because they are consumed by the forwarding ASIC's physical registers without sending them to the CPU.
  - Dot1x that uses 0180c2000003 is disabled by the Cisco ME 3800 and ME 3600 switches. This functionality is the same as in previous releases.
  - L2PT tunneling for the reserved MACs is not supported since the reserved MACs do not have known link types. Reserved MACs tunneled with 0180C200000B are replaced to ensure packets egress.
  - The LinkOAM, ELMI, and ESMC protocols are considered to be "L2PT peer" even if the L2PT CLI is not applied on the interface. Unlike other protocols, L2PT code assumes it to be drop. This is done to avoid L2PT peer configuration for LinkOAM, ELMI, and ESMC since these protocols previously worked without L2PT configurations.
- Downgrading to Cisco IOS 15.2(2)S from I/O Mode 3 is not supported. Ensure you are in I/O Mode 2 or I/O Mode 1.

## Open Caveats

The following sections provide information about open caveats:

- [Open Caveats in Cisco Release 15.3\(1\)S, page 15](#)
- [Open Caveats in Cisco Release 15.3\(1\)S1, page 16](#)
- [Open Caveats in Cisco Release 15.3\(1\)S2, page 17](#)

## Open Caveats in Cisco Release 15.3(1)S

- CSCuc21897

On the Cisco ME3600X-24CX, the Entity MIB is not responding for the T1/E1 controller ports. Conditions: When you walk entitymib OID for the entPhysicalEntry, no T1/E1 ports details are returned.

Workaround: None.

- CSCuc72457  
Buffer manger lockup occurs on the Cisco ME 3600X-24FS-M when two ports on the Cisco ME 3600X-24FS-M (GI0/13,14) are configured as Xconnects to two ports on the Cisco ASR 9000.  
Conditions: None, as this is a hardware failure (QDR parity error).  
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 tracebacks. Memory leaks are also observed.  
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.
- CSCub33943  
Platform assert failures and tracebacks are observed upon modifying EFP to a different EVC BD configuration.  
Conditions: Observed only when the EFP is changed to a different EVC BD configuration.  
Workaround: None.

## Open Caveats in Cisco Release 15.3(1)S1

- 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, the traffic received from the Spoke VC gets punted to the CPU (Software Forwarded).  
Workaround: None.
- CSCuc14594  
There is a drop in static pseudowires over mpls-tp traffic.  
Conditions: By default, static pseudowires are configured in vc\_type4 mode. Since vc\_type4 was not configured correctly, there was a drop in traffic.  
Workaround: This behavior can be changed by setting interworking in pw-class as Ethernet, as follows:  

```
pseudowire-class static-pw-interworking
  encapsulation mpls
  interworking ethernet
```
- CSCuc47879  
Removing channel group configuration on a CEM controller causes device to hang in a particular scenario.  
Conditions: This issue occurs with the following steps:
  1. Configure CEM group (CESoPSN or SAToP) on a controller.
  2. Configure channel group on this controller with same timeslots used in (1) for CEM group.
  3. Remove channel group configured in (2).



- Workaround: Soft or hard reboot the device.
- CSCue01649  
CPU errors are seen with (\*, G/M) entries with ACL.  
Conditions: This issue is seen on ME 3600X-24CX boxes in mode 3.  
Workaround: Operate the box in mode 2.
  - CSCue02251  
When doing archive download to upgrade or downgrade a software version, old image present in the board is not getting deleted or displayed.  
Conditions: This issue occurs during "archive download."  
Workaround: No specific condition.
  - CSCue18541  
ARP does not pass for Tunneled VLANs.  
Conditions: IP ARP inspection is enabled on a switch where dot1q tunnel is configured.  
Workaround: Remove ARP inspection.
  - CSCue20246  
Executing "no ip icmp redirect" globally does not result in ICMP redirects to stop.  
Conditions: None. This command is not functioning as expected.  
Workaround: None.
  - CSCue30168  
Ping failure occurs upon path switchover from EVC to routed PW.  
Conditions: When MAC move occurs from EVC to routed PW, ping fails  
Workaround: Clear MAC address table.
  - CSCue38489  
ICMP replies getting duplicated on ME3600 switch.  
Conditions: Create service instances on port channel interfaces on ME3600 in a topology shown below:  
IXIA---7600(Te2/1-2)====(PO1)====(Te0/1-2)ME3600(Gi0/4-5)====(PO2)====(Gi1/0/25-26)  
SW3750-----IXIA  
Workaround: None.

## Open Caveats in Cisco Release 15.3(1)S2

- CSCtz51263  
An additional 4 bytes are added into the calculation of the MTU. Packets are punted to the CPU even if the size of the packet is under the configured MTU.  
Conditions: Observed on the Cisco ME 3600X, with the MPLS label swap situation.  
Workaround: Set the MTU to 4 bytes or more.
- CSCub11348  
Broadcast traffic flows over the standby spoke VC and then gets punted.

Conditions: Traffic comes over the core VCs and 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 tracebacks and memory leaks.

Conditions: Observed with the Cisco ME 3600X, where a multicast stream can be received on any type of interface (L2/L3).

Workaround: None.

- CSCuc36156

DWDM SFP+ are supported, but when inserted, the switch does not recognize the DWDM.

Conditions: When a DWDM SFP+ is present on the switch.

Workaround: None.

- CSCuc47879

Removing channel group configuration on a CEM controller causes device to hang in a particular scenario.

Conditions: This issue occurs with the following steps:

1. Configure CEM group (CESoPSN or SAToP) on a controller.
2. Configure channel group on this controller with same timeslots used in (1) for CEM group.
3. Remove channel group configured in (2).

Workaround: Soft or hard reboot the device.

- CSCud50038

Include VPLS VC ID information in the mac flap notification messages.

Conditions: VPLS VC information is missing in mac-flap messages.

Workaround: None.

- CSCud94899

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

Conditions: Create a port-channel using gig 0/1.

Workaround: None.

- CSCue10562

MPLS PW ping fails.

Conditions: Observed during the upgrade from 3.7.2 to 3.8.1.

Workaround: None.

- CSCue11706

Tracebacks related to CPU hogs on reload. Also observed on shut/no shut of interfaces.

Conditions: Creating a large number of EFPs (1k or more) on a single interface leads to the CPU hog.

Workaround: None.

- CSCue20246  
Executing the **no ip icmp redirect** command globally does not result in stopping ICMP redirects.  
Conditions: None.  
Workaround: None.
- CSCue30311  
Router crash on configuring VLAN first and reconfiguring the policy-map.  
Conditions: Observed when the QoS policy-map applied on the switchport interface is reconfigured or modified after the addition of a VLAN globally.  
Workaround: Configure the VLAN and wait until the CPU is normal, then modify the policy-map.
- CSCue52985  
The new policy-map configuration does not take effect. Traffic is still marking as per the old configuration.  
Conditions: Observed when dynamically confirm action configuration is deleted from the policer configuration.  
Workaround: Remove the service-policy from the interface/service instance and add it back.
- CSCue53009  
LDP flaps observed.  
Conditions: Packet drops observed in platform counters.  
Workaround: None.
- CSCue94397  
Trust port configuration will be invalid on DHCP snooping over EVC. the DHCP discover request cannot be snooped correctly and will be dropped on EVC in L2 flat environments.  
Conditions: Observed when configuring in new interface regarding BD of trust port, and when reloading after saving configuration.  
Workaround: None.
- CSCuf21377  
PMIPv6 control traffic is process switched on by the MPLS PE router. Some PMIPv6 control traffic is being dropped.  
Conditions: Switch configured as MPLS PE is transiting PMIPv6 traffic.  
Workaround: None.
- CSCuf30192  
Multicast traffic stops being forwarded when a Mrouter (SVI) VLAN is shut, and the incoming and outgoing interface are on the same VLAN.  
Conditions: IGMP snooping has to be enabled, SVI has to be acting as an Mrouter, and when this Mrouter is shut, traffic should still flow because L2 connectivity is up. But an outage is observed.  
Workaround: Perform an IGMP snooping enable, then disable.
- CSCuf43673  
A system crash occurs on the Cisco ME 3600X switch and error messages appear.

Conditions: Observed after changing the route-map on the route-reflector that establishes the switch. The Cisco ME 3600X is a route-reflector-client. The route-map setting that you change on the route-reflector is the output route-map for the other route-reflector-client, not for the Cisco ME 3600X.

Workaround: None.

- CSCuf73923

CLI command to get PHY info without interface option is being rejected.

Conditions: Observed when the **PHY info** CLI command is entered without an interface option.

Workaround: Specify the interface option in order to get the PHY information.

- CSCuf85356

The Cisco ME 3600X tags packets on the native vlan of a .1Q trunk if the packets have been routed. Local generated packets will go untagged, and packets that have only been switched through the Cisco ME 3600X will go untagged. But if the packet enters the Cisco ME 3600X on another VLAN and is routed to the destination VLAN, it will be tagged when leaving on a .1Q trunk.

Conditions: None.

Workaround: None.

- CSCuf98310

CPU utilization stuck at 100 percent.

Conditions: Observed upon a periodic shut and no shut of the 10 GigE interface.

Workaround: Power cycle the switch.

- CSCug08514

When changing the policer PIR on a system with high TCAM usage, the CPU spikes and the configuration change can take several minutes.

Conditions: Observed in cases of high TCAM usage.

Workaround: None.

- CSCug22139

When an ACL with the **range** command is used for QoS, tracebacks are observed.

Conditions: 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

When a Y1731 is active on flexlink uplink ports, no measurements are done when the active flexlink port is down and the standby takes over as active.

Conditions: Observed when UP MEP is configured, flexlink is configured on uplink ports, and Y1731 SLM is active on flexlink.

Workaround: None.

- CSCug33146

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

Conditions: VLAN up trigger to multicast has to be missed. This is a very rare case, but could happen in an environment where VLAN up and down is common.

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

- CSCug33345  
ARP resolution fails with DAI enabled.  
Conditions: Observed after enabling DAI on another VLAN.  
Workaround: Enable the DAI on the VLAN of interest.
- CSCug33386  
Frame loss observed when configuring an existing class-map to a new service instance. The frame loss is observed on the existing service instance.  
Conditions: Observed if the class-map has the same value as the SET value (such as SET DSCP and SET QOS group).  
Workaround: None.
- CSCug33828  
After reloading the Cisco ME 3600X, part of the configuration presented below disappears, causing part of the network to not function until those commands are re-added to configuration:

Before reload:

```
ME-3600X#sh running-config | b bridge-domain
bridge-domain 1001
  member GigabitEthernet0/1 service-instance 1001
  member GigabitEthernet0/2 service-instance 1001

interface GigabitEthernet0/1
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1001 ethernet

interface GigabitEthernet0/2
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1001 ethernet
```

After restart:

```
Bridge-domain 1001 created
VLAN 1001 does not exist, creating vlan
  member GigabitEthernet0/1 service-instance 1001
  ^
% Invalid input detected at '^' marker.

  member GigabitEthernet0/2 service-instance 1001
  ^
% Invalid input detected at '^' marker.

ME-3600X#sh running-config | b bridge-domain
bridge-domain 1001

interface GigabitEthernet0/1
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1001 ethernet

interface GigabitEthernet0/2
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1001 ethernet
```

Conditions: Observed upon reload.

Workaround: None.

- CSCug34597

After TCAM has been exhausted, even after TCAM resources have been removed, a service policy cannot be applied. The TCAM clean up is not functioning properly.

Conditions: Observed on the Cisco ME 3600X after exhausting the TCAM.

Workaround: Reload the switch.

- CSCug37183

Ping fails beyond the connected PE devices.

Conditions: Observed only when the dot1q tag that is matched under EFP is different from the configured bridge domain for the same service instance.

Workaround: Ensure that the bridge domain, service instance, and dot1q tag are the same, then the ping should work fine beyond the connected PE devices.

- 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: 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.

- CSCug50399

When sending broadcast traffic via a span destination port, the span destination port forwards the traffic, and other ports of the Cisco ME 3800X receive it.

Conditions: None.

Workaround: None.

- CSCug50678

Traffic is not switching to the protect path.

Conditions: With MPLS TP in the core, traffic is not switching to the protect path upon changing the outlink number.

Workaround: None.

- CSCug51255

Traffic is not switching to protect path.

Conditions: With MPLS TP in the core, traffic is not switching to protect path upon bringing down the active path with the interface shut at the mid point.

Workaround: None.

- CSCug53660

On the Cisco ME 3600X or ME 3800X, it takes 3.5 seconds for traffic to converge on the SVI when preemption is forced back to the active flexlink port.

Conditions: Observed when flexlink is configured in non-VLB mode and preemption mode is configured as forced.

Workaround: None.

- CSCug58922  
TE FRR protected link failure convergence is more than 50 msec.  
Conditions: Remove end failure of the protected link.  
Workaround: Use BFD aware TE FRR and carrier delay on the protected link, which will improve the convergence.

## Resolved Caveats

The following section provides information about resolved caveats:

- [Resolved Caveats in Cisco Release 15.3\(1\)S1, page 23](#)
- [Resolved Caveats in Cisco Release 15.3\(1\)S2, page 30](#)

### Resolved Caveats in Cisco Release 15.3(1)S1

- CSCtq77861  
Polling the BRIDGE-MIB for VLAN data other than VLAN 1 times out on 3600X and 3800X switches  
Conditions: This issue occurs with any 3600X or 3800X switch because SNMP contexts for each VLAN are not created.  
This enhancement is filed to track the addition of support for this functionality.  
Workaround: None.
- CSCts82886  
DHCP snooping binding is not established on EVC BD trusted port.  
Conditions: When DHCP snooping is enabled on one or more VLANs and EVC BD is configured on trusted port connected towards SP network/DHCP server, client does not receive IP address, and DHCP snooping binding is not established.  
Workaround: None. Only switchport can be configured as trusted port.
- CSCtz11548  
Confirm and Exceed action counters in the show policy-map interface are not getting cleared with scale configurations on doing clear counters.  
Conditions: This issue occurs when doing clear counters.  
Workaround: Remove the policy-map and add it back.
- CSCtz19724  
When an ACL with more than 1K ACEs is applied, the ACL does not come into effect and any error is not thrown too.  
Conditions: This issue occurs when applying an ACL with greater than 1024 ACEs. The ACL does not get applied and TCAM write does not happen. This is expected as limit on number of ACEs is exceeded. However, no error message is shown on console that it has failed.  
Workaround: No workaround. ACEs should not exceed 1K.
- CSCtz35089

Traffic burst differences from 10G.

Conditions: Traffic burst from 10G connected to ASIC1 is twice compared to ASIC0.

Workaround: None.

- CSCtz46946

Traceback is seen on creating TE tunnel with 6PE/6VPE configuration. No functionality impact.

Conditions: Configure 6PE/6VPE, create TE tunnel with auto-route announce

Workaround: None.

- CSCtz77011

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

Conditions: This issue occurs with pair or ME switches with layer 2 port-channel in between and 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.

- CSCua39229

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

Conditions: Configs - 'input 1pps 0/0' on master and 'output 1pps 0/0' on slave are not deleted when PTP is unconfigured.

Workaround: Need to unconfig 'input 1pps 0/0' or 'output 1pps 0/0' before unconfiguring PTP.

- CSCua98805

Traceback is seen at adjmgr\_free\_met.

Conditions: On defaulting an attachment interface having L2PT configured and used for VPLS traceback is seen.

Workaround: None.

- 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: 1:1 (one active and one standby) scenario where the hot standby converges to active.

Workaround: None.

- CSCub64331

10m reference to SETS goes to OOR on connecting 1pps input.

Conditions: Connect both 10m and 1pps inputs.

Workaround: Have only 10m connected. The SETS goes to locked state without any issue. 1pps input does not work with this defect.

- CSCub64585

EoMPLS link stays down, although VC is up.

Conditions: This issue is seen when changing encapsulation from default to dot1q and vice versa

Workaround: None.

- CSCub68933



Incorrect MAC learning is observed over pseudowires that are part of HVPLS, causing a traffic failure.

Conditions: This symptom is observed when VPLS auto discovery is in use with MPLS over SVI in the core. This issue is also seen with LDP-based VPLS when split horizon-enabled pseudowires are configured after the non-split horizon-enabled pseudowires.

Workaround: None.

- CSCub76041

After defaulting the port-ch and applying back the configurations on it, eth serv instances are down.

Workaround: shut and no shut on the port-ch brings the EFPs up, Or, configure the port channel command by command instead of copy pasting the configurations

- CSCub89774

VPLS Interworking Type is shown as incorrect.

Conditions: It is shown correctly on **show mpls l2 vc binding** output.

It is shown incorrectly on **show mpls l2 vc detail** output.

Workaround: Issue **clear mpls ldp neighbour** after issuing **interworking vlan.**

- CSCuc03501

IS-IS over HDLC serial link is not up.

Conditions: Configure a serial interface and assign an IP address to it. Configure IS-IS Routing Protocol over a serial interface

Workaround: None.

- CSCuc59049

The Cisco ME 3800X crashinfo files may be corrupted.

Conditions: A crashinfo file is created when there is a crash.

Workaround: Gather console logs and syslogs to help troubleshoot crashes.

- CSCuc59105

The Cisco ME 3600X/ME 3800X may crash when running the following command: show platform qos policer cpu x x.

Conditions: Observed only when run through an SSH session and with AAA configured.

Workaround: Run the commands through telnet or console.

- CSCuc59765

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

Conditions: Soaking over a prolonged period of time.

Workaround: None.

- CSCuc76515

Xconnect fails to negotiate to the correct vc-type on reload.

Conditions: This symptom is seen in vc-type4 session.

Workaround: Clear Xconnect peer.

- CSCuc79161

Memory leaks observed. The PI front-end pseudoport is not deleted when the Xconnect is removed, which causes the memory leak. It is because PD returns BDOMAIN\_PP\_FAILED to PI when pp\_engine\_context is a NULL pointer.

Conditions: Flapping the interface, keeping the setup idle, and executing CLI clear Xconnect all results in memory leaks.

Workaround: None.

- CSCuc80520

EVC ingress counter becomes zero after delete/add "ethernet service" configure.

Conditions: This symptom is seen while EVC QinQ use topology.

Workaround: Issue shut/no shut port-channel interface.

- CSCuc90580

Ping fails over a routed PW setup.

Conditions: SVI-based MPLS uplink.

Workaround: Disable MAC learning.

- CSCuc93165

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

Conditions: Add and delete user-defined class-map.

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

- CSCuc93252

Traceback observed after executing "archive download" command is executed in ME 3600X-24CX.

Conditions: None.

Workaround: None.

- CSCuc94983

The ConPE node crashes intermittently after soaking it with events.

Conditions: Rigorous flapping of the core.

Workaround: Stabilize the core network.

- CSCud01498

SAToP/CESoPSN traffic has no priority in MPLS core.

Conditions: CEM pseudowire traffic has EXP = 0 in the MPLS core which gives no priority. There is no service-policy support to mark exp as well.

Workaround: None.

- CSCud01508

Non-ip packets are accounted in class-map having "match ip any any" in the access-list

Conditions: When an ip qos acl match is applied, even non-ip packets like arp etc. also get classified into that class.

Workaround: None.

- CSCud01781

Traffic is not blocked if a new level is configured after the existing level is still violated.

Conditions: Change the existing level (for example, 15%) to a new level (for example, 20%).

Workaround: None.

- CSCud06908

This issue occurs if ME3800X and 7600 are working as PE devices and if they have multiple core connections between them.

If one of the core interface between ME3800X and 7600 and the attachment circuit (AC) is bounced simultaneously on ME3800X, the VPLS status on ME3800X shows 'up' but it shows 'down' on 7600.

Conditions: There should be multiple connection between core devices.

Workaround: Bounce attachment circuit on 7600 to resolve the issue

- CSCud09627

Error messages similar to the following: “npm\_intfman\_get\_el3idc\_vlan\_index:interface el3id handle is NULL” are observed on the console.

Conditions: Observed upon performing the following commands:

```
no mpls traffic-eng tunnels
mpls traffic-eng tunnels
clear ip bgp *
```

Or, upon performing IM OIR on the peer end.

Workaround: None.

- CSCud11453

Traceback appears in console:

```
:39:23.127: %IPV6_ROUTING-3-RIB: ipv6_is_addr_ours called for link-local address with
wrong tableid -Process= "NCEF ADJ Refresh bg process", ipl= 0, pid= 84
-Traceback= 6FAF20z 10C1A44z BA391Cz 2AF5C04z 2BFFC6Cz 2C566CCz 2C519B8z
```

Conditions: This issue occurs when enabling IPv6.

Workaround: None. Does not have functional impact.

- CSCud17700

On executing "sh inv" command when SFP-10G-LR SFP-10G-SR present in a Cisco ME 3600/ME 3800 box, the Description is missing.

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

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 SPF 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 exists in 15.2(4)S1.

Workaround: None.

- CSCud26145

ME3600X: Unsupported L4 type in QoS ACL can be applied to a port.

- CSCud28879

IGMP snooping pruning port even if report arrives as a reply to the GSQ. (GSQ is sent when a leave comes on a port.)

Conditions:

1. IGMP general-query (GQ) comes during the time when snooping last-member-query (GSQ) timer is on.
2. GQ timer expires before the GSQ timer.
3. A report comes before the GQ timer expires.
4. No reports are received after the GQ timer expires.

For the issue to be seen, all the above four conditions have to be true.

Workaround: None.

- CSCud29000

Traffic with wrong tag is sent on dynamically modifying the rewrite tag.

Conditions: On dynamically changing the tag to be pushed, device sends traffic with previously configured tag.

Workaround: Remove the service instance and reconfigure with new rewrite tag to be pushed.

- CSCud46291

Conditions: Exception is seen when an unsupported SFP with invalid EEPROM content is inserted and replaced with a supported SFP when the interface is in error-disabled state.

Workaround: Use a supported SFP.

- CSCud50326

Tracebacks seen @adjmgr\_l3\_delete\_nh.

Conditions: This issue occurs when configuring VFI Xconnect and enabling PIM under SVI. Traceback is seen on removing ip address under SVI.

Workaround: None.

- CSCud50354

Unsupported SFP does not get recognized on ME 3800X, ME 3600X, and ME 3600X-24CX.

Conditions: This issue occurs when eeprom is not correctly programmed according to SFF8472 standard.

Workaround: None.

- CSCud63907

To enable PTP, reload the box and set the variable ENABLE\_PTP\_CPU to 1 in the switch prompt.

Workaround: Always set ROMMON variable ENABLE\_PTP\_CPU to 1.

- CSCud68830

End to end L3 traffic is affected if the host queue (cpu queue 2) increments continuously at high rates (2000 packets/s and above).

Conditions: End to end L3 traffic is affected if the host queue (cpu queue 2) increments continuously at high rates (2000 packets/s and above).

Workaround: None.

- CSCud75003

CoS inner value gets changed on marking with CoS in egress on QinQ service instance without rewrite.

Conditions: QinQ service instance without rewrite operation.

Workaround: None.

- CSCud83056

PTP session is stuck in HOLDOVER after PTP unconfig/config on master.

Conditions: Need to unconfig/config PTP on master.

- 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 flap on every device that are on the path through which the BPDU traverses.

Workaround: The workaround to the above issue is to apply split horizon at the bridge-domain where the MAC flaps happen.

- CSCud90770

Packets stopped looping back on dynamically attaching service-policy when loopback session is active.

Conditions: It is seen only on attaching policy-map after starting the loopback session.

Workaround: None.

- CSCud90827

Conform and exceed counters are taking more time to get updated properly.

Conditions: The issue is seen in presence of ELB session with QoS enabled.

Workaround: None.

- CSCud95416

QoS Configuration failed error occurs even when the policy with shaping/bw/priority is attached to output direction.

Conditions: This issue is seen only when the policy is attached with loopback session active.

Workaround: Attach the policy before starting the loopback session.

- CSCud96997

ip sla does not show any statistics, and raw db is also not populated.

Conditions: When core interface is a switch port trunk, this issue occurs.

Workaround: None.

- CSCud97289

PTP slave is not able to start session with master.

Conditions: PTP session not started if slave's and master's loopback IP addresses are in same subnet.

- Master loopback address: <ipaddress>
- Slave loopback address: <ipaddress>

Workaround: Configure slave's and master's loopback IP addresses in different subnets.

- CSCue00690

User-defined classes in the policy-map applied on EVC with rewrite push is not supported. This configuration gets accepted on an in certain conditions.

Conditions: This happens when the QoS policy is applied first to the EFP, and then the bridge domain configuration is applied.

Workaround: None.

- CSCue01505

QoS memory chunk leaks are observed on certain scenarios of ELB QoS.

Conditions: This issue is observed on defaulting the interface applied with QoS policy, flapping the interface, and stopping the loopback session

Workaround: None.

- CSCue11488

Linkoam does not work without the l2protocol peer configuration on an untagged EVC.

Conditions: This is a regression caused by CSCud63960 commit for the linkoam flow.

Workaround: None.

## Resolved Caveats in Cisco Release 15.3(1)S2

- CSCuf25555

Policy-based routing stops working after the switch reloads.

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

Workaround: Remove and reconfigure the route-map.

- CSCud22527

On the Cisco ME 3600X, when mac security is configured on an EFP port, the traffic received on this EFP and destined to one mac addressed learned on the same EFP will be bounced back to the EFP.

Conditions: Traffic is NOT bounced back in the following conditions:

- Mac security is removed
- A split-horizon group is configured on the EFP
- The EFP is replaced by a legacy L2 trunk

Workaround: None.

- CSCud92714

When the port-channel is deleted and created again, the max MTU can not be set up.

Conditions: Delete the port-channel and re-create it.

Workaround: Reload the device.

- CSCue30590

Packet loss is observed over pseudowire and high CPU.

Conditions: 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.

- CSCue01649

CPU errors observed with (\*, G/M) entries on the ACL.

Conditions: Observed on Cisco ME 3600X switches operating in Mode 3 or Mode 4.

Workaround: Operate the Cisco ME 3600X switch in Mode 2.

- CSCue89385

Traffic from routed VPLS does not trigger ARP.

Conditions: 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.

- CSCue62031

The Cisco ME 3600/3800X switches may reload when a BGP session flaps.

Conditions: Observed only if there is more than one BGP neighbor configured on the switch.

Workaround: None.

- CSCue10844

Classification does not work properly.

Conditions: Observed only if there are classes based on ACL match and normal DSCP match. Only the ACL class will classify properly, and other classes do not work.

Workaround: None.

- CSCue61393

Ingress classification based on a numbered IP ACL does not work correctly.

Conditions: If an ingress QoS policy contains a match based on a numbered ACL, classification does not work and the actions do not take effect.

Workaround: Use a named ACL instead of a numbered ACL for the match.

- CSCue96478

A stall is received in the ETSEC driver. The ping drops on controller interface Gi0.

Conditions: None.

Workaround: Perform a shut/no shut on the Gi0 interface.

- CSCuf16072

While attempting to upload the image using the command **archive upload-sw**, the system was unable to create the temp directory. ramfs:update occurred, and the image failed to upload.

Conditions: None.

Workaround: Use copy flash: tftp: instead.

## 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-24CX switch:

[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—2013 Cisco Systems, Inc. All rights reserved.

