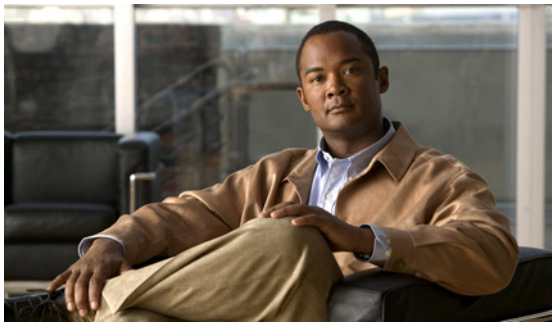

Release Notes for the Cisco ME 3800X and ME 3600X Switch, Cisco IOS Release 15.1(2)EY and Later Releases

January 22, 2013

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

- Cisco IOS Release 15.1(2)EY
- Cisco IOS Release 15.1(2)EY1a
- Cisco IOS Release 15.1(2)EY2
- Cisco IOS Release 15.1(2)EY2a
- Cisco IOS Release 15.1(2)EY3
- Cisco IOS Release 15.1(2)EY4

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

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

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 5.
- If you are upgrading to a new release or a different image, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

For the complete list of Cisco ME 3800X and ME 3600X switch documentation, see the "Related Documentation" section on page 72.

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

http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

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

Contents

Hardware Supported

Table 1 Supported Hardware

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

Software Licenses and Features

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

The ME 3600X supports these licenses:

- Metro IP access is the universal image.
- Advanced Metro IP access license.

- 10 Gigabit Ethernet upgrade license—enables 10 Gigabit Ethernet on the SFP+ uplink ports.

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

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

- Metro Ethernet services is the universal image.
- Metro IP 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 4.

To install a software image, see the "Upgrading the Switch Software" section on page 5 and the "Working with the Cisco IOS File System, Configuration Files, and Software Images" chapter in the software configuration guide.

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

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

Table 2 ME 3600X Supported Features per License

Metro IP Access (Universal Image)	Advanced Metro IP Access license
• Basic Layer 2 features (including 802.1Q) • Ethernet Virtual Circuits (EVCs) • IPv4 routing—RIP, OSFP, EIGRP, IS-IS, and BGP • Bidirectional Forwarding Detection (BFD) • Multicast routing —PIM, DM, SSM, and SSM mapping • Ethernet Operations, Administration, and Maintenance (OAM)—802.1ag, 802.3ah, and E-LMI • Multiple Spanning Tree Protocol (MSTP), Resilient Ethernet Protocol (REP), and Flex Links • Synchronous Ethernet 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	• 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 License Scaling and template

Supported feature	Metro IP Access		Advanced Metro IP Access	
SDM Templates	**Default**	**IPv4**	**Default**	**IPv4**
MAC addresses	8 K	8k	16 K	16 K
IPv4 routes	20 K	24K	20 K	24 K
IPv4 routing groups	1 K	1K	1 K	1 K

Table 3 ME 3600X License Scaling and template (continued)

Supported feature	Metro IP Access		Advanced Metro IP Access	
IPv6 routes	5 K	4 K	5 K	3 K
Multicast groups	1 K	1 K	1 K	1 K
Bridge domains	4 K	4 K	4 K	4 K
ACL entries	2 K	2 K	2 K	2 K
IPv4 QoS classification	4 K	4 K	4 K	4 K

Table 4 ME 3800X Supported Features per License

Metro Ethernet Services (Universal Image)	Metro IP Services license	Metro Aggregation Services license
• Basic Layer 2 features (including 802.1d and 802.1Q) • EVCs • Ethernet OAM—802.1ag, 802.3ah, and E-LMI • MST, REP, Flex Links • Synchronous Ethernet with Ethernet Synchronization Messaging Channel (ESMC)	• All features in the Metro Ethernet Services image • IPv4 routing—RIP, OSFP, EIGRP, IS-IS, and BGP • BFD • Multicast routing—PIM, DM, SSM, and SSM mapping • Multi VRF-CE with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)	• All features in the Metro IP Services license • MPLS • MPLS traffic engineering and Fast Reroute • MPLS OAM • MPLS VPN • EoMPLS • Pseudowire redundancy • 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
MAC table addresses	64 K	128 K	32 K	64 K	128 K	256 K
IPv4 routes	1 K	1 K	42 K	80 K	24 K	32 K
IPv4 multicast groups and routes	0	0	2 K	4 K	2 K	4 K
IPv6 routes	500	500	21 K	40 K	12 K	16 K
Layer 2 multicast entries	2 K	4 K	2 K	2 K	2 K	4 K
Bridge domains	4 K	4 K	2 K	2 K	4 K	8 K
ACL entries	4 K	8 K	4 K	8 K	4 K	16 K
IPv4 QoS classification	4 K	4 K	4 K	4 K	4 K	24 K

Table 6 ME 3800X Scaled Metro Aggregation templates

Supported feature	Scaled Metro Aggregation Service License		
SDM Templates	**Default**	**VPNv4**	**VPNv4+IPv6**
MAC table	256 K	256 K	256 K
IPv4 routes	32 K	80 K	80 K
IPv4 routing groups	4 K	8K	2 K
IPv6 routes	16 K	8 K	40 K
Multicast groups	4 K	4 K	2 K
Bridge domains	8 K	4 K	8 K
ACL entries	16 K	4 K	4 K
IPv4 QoS classification	24 K	12 K	12 K

Upgrading the Switch Software

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. The image is stored on the system board flash device (flash:).

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

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The software installation procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 7 Cisco IOS Software Image Files

Filename	Description
me380x-universal-tar.151-2.EY.tar me380x-universal-tar.151-2.EY1a.tar me380x-universal-tar.151-2.EY2.tar me380x-universal-tar.151-2.EY2a.tar me380x-universal-tar.151-2.EY3.tar me380x-universal-tar.151-2.EY4.tar	Cisco ME 3800X universal images.
me380x-universalk9-tar.151-2.EY.tar me380x-universalk9-tar.151-2.EY1a.tar me380x-universalk9-tar.151-2.EY2.tar me380x-universalk9-tar.151-2.EY2a.tar me380x-universalk9-tar.151-2.EY3.tar me380x-universalk9-tar.151-2.EY4.tar	Cisco ME 3800X universal cryptographic images. These images have the Metro Ethernet features plus Kerberos and SSH.
me360x-universal-tar.151-2.EY.tar me360x-universal-tar.151-2.EY1a.tar me360x-universal-tar.151-2.EY2.tar me360x-universal-tar.151-2.EY2a.tar me360x-universal-tar.151-2.EY3.tar me360x-universal-tar.151-2.EY4.tar	Cisco ME 3600X universal images.
me360x-universalk9-tar.151-2.EY.tar me360x-universalk9-tar.151-2.EY1a.tar me360x-universalk9-tar.151-2.EY2.tar me360x-universalk9-tar.151-2.EY2a.tar me360x-universalk9-tar.151-2.EY3.tar me360x-universalk9-tar.151-2.EY4.tar	Cisco ME 3600X universal cryptographic images. These images have the Metro IP access features plus Kerberos and SSH.

Installing Software Images and Licenses

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

Before installing your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

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

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

Step 1 Use Table 7 on page 6 to identify the file that you want to download.

Step 2 Locate the software image file:

a. If you are a registered customer, go to this URL and log in.

http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

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

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

c. Navigate to your switch model.

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

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

Step 3 Download the image to a TFTP server and make sure that the server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch by entering this privileged EXEC command:

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

- For **//***location*, specify the IP address of the TFTP server.
- For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
- The **/overwrite** option overwrites the software image in flash memory with the downloaded one.
- The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/image-name.tar
```

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

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

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

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

```
Switch# show boot
BOOT path-list      :
flash:/me380x-universal-mz.151-2.EY/me380x-universal-mz.151-2.EY.bin
Config file         :    flash:/config.text
Private Config file : flash:/private-config.text
Manual Boot         : no
HELPER path-list    :
```

Step 8 Save the configuration and reload the switch.

```
Switch# reload
```

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

Step 1 Copy the license file to flash or TFTP.

Step 2 Enter 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 a scaled license, install the scaled license

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

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

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

```
Switch# reload
```

Installation Notes

You can assign IP information to your switch by using these methods:

- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Software Features

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

Note The IPv6 Provider Edge (6PE) and IPv6 VPN Provider Edge (6VPE) features are not supported in this release.

Important Note

- Switch Port Analyzer (SPAN) is not supported.

Resolved and Open Caveats

The following sections provide information on resolved and open caveats:

- Open Caveats for Cisco IOS Release 15.1 (2) EY, page 9
- Resolved Caveats for Cisco IOS Release 15.1 (2) EY, page 13
- Resolved Caveats for Cisco IOS Release 15.1 (2) EY1a, page 17
- Resolved Caveats for Cisco IOS Release 15.1 (2) EY2, page 38
- Resolved Caveats for Cisco IOS Release 15.1 (2) EY2a, page 59
- Resolved Caveats for Cisco IOS Release 15.1 (2) EY3, page 60
- Resolved Caveats for Cisco IOS Release 15.1(2)EY4, page 67

Open Caveats for Cisco IOS Release 15.1 (2) EY

- CSCtf02910

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

  Packets punted to CPU for any reason after Ingress QoS processing, are not classified correctly at Egress QoS, and are not re-marked as per input QoS "set" action.

  This issue only affects incoming data packets which need to be punted to CPU for further processing and then sent out of another port, for example packets with "IP options."

CPU punted packets for different cases are handled a bit differently in the ASIC. The details of retrieving and assigning internal resources are being worked at. This information is not readily available currently for all cases in the CPU punt path, and as a result these packets do not have the necessary information once they leave the CPU and egress out of an interface. Hence, these are not classified correctly in an output policy map, nor are marked according to any "set" action in the input policy map class that these match. These packets match in the correct class in an input policy map, but match class-default in an output policy map.

Workaround: None. CPU punted packets are not re-marked as per input policy, nor classified at egress.

- CSCto33293

  Router forwarding bpdu data on STANDBY PW after primary failover.

  Workaround: None.

- CSCto61243

  Platform assert failures on flapping 10G interface with EBGP sessions.

  Error messages with tracebacks appear on the console after flapping of interfaces happen. The error message states that the di_index cannot be found.

  When interfaces are shut, forwarding stops, therefore destination indices (di_index) are set to illegal values causing the error message to be displayed. The error messages do not cause any traffic outages.

  Workaround: None.

- CSCtq29544

  QoS: Incorrect removal of efp service-policy on adding port-shaper.

  If a HQoS policy-map is applied on an EVC, parent bandwidth percent of 10%, child total bandwidth of 350mbps, when the port_shaper with 500 Mbps at the port level is added, the EVC policy-map gets removed. Ideally the port_shaper configuration should be rejected when there is an error in the configuration.

  Workaround: Detach the policy-map, create a valid configuration, and attach to the interface.

- CSCtq29611

  QoS: Stale QoS entry in the forwarding ASIC on dynamic removal of child.

  In a HQOS policy, packets are still subjected to child policy even though its removed from parent class.

  When attempting to remove a child policy under a class, the child-policy is not removed from hardware. This means that the traffic is subjected to actions in the child service policy even though its removed from running-config.

  Workaround: Detach and reattach the policy.

- CSCtq74682

  SPF scheduled twice when the **max-metric** command or **no max metric** command is issued.

  Workaround: None.

- CSCtq74742

  ACL with tcp established drops packets intermittently on ME3600X.

  Workaround: Apply ACL with permit tcp to any established on ingress direction.

- CSCtq94357

  The output of the **show platform ip multicast groups 192.0.2.254 details** command does not display the output based on the group address on licensed image, it show the output for all groups at one time. Terminal length is also not working.

  The issue is seen only in the licensed image. It works correctly in the universal image.

  Workaround: None.

- CSCtq97559

  On issuing the **ip multicast boundary** command, transient traffic loss was observed. This also occurs for packet streams that are permitted in acl.

  Workaround: None.

- CSCtr32787

  PW-R: Observing traceback @ CHUNKBADMAGIC, Process= "Collection process."

  The following message appears when switching the pseudowire from primary to backup:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 1391E3D4
  chunkmagic D0D0D0D chunk_freemagic D0D0D0D -Process= "Collection process", ipl= 0,
  pid= 210
  ```

  Workaround: None.

- CSCtr42803

  Configuration is not rejected when the user attaches vfi to Bridge Domain which has 60 EFPs configured.

  Pseudowire configuration (EoMPLS/VPLS) is not rejected even when number of EFPs configured in the bridge-domain+existing Pseudowires equals 64. The maximum supported number of pseudowire+EFPs on a bridge-domain is 64.

  Workaround: None. The configuration is unsupported.

- CSCtr47362

  Multiple flap of core results in adj failures followed by forwarding ASIC asserts

  Rigorous flapping of mpls uplinks combined with use of clear ip route command and clear mpls ldp neighbor command results in the following message appearing on the router console:

  ```
  platform assert failure: 0: ../src-nile/src-asic-nile/nile_adjmgr.c: 9533:
  adjmgr_get_fid_index
  ```

  Workaround: None.

- CSCtr56009

  SVI link stays up even when the corresponding vlan has been shut down.

  Workaround: None.

- CSCtr56483

  Tracebacks and Asserts upon removing and adding Vlans from database

  Tracebacks is thrown when there is a PW on vlan/SVI, and vlan is deleted, then added back.

  Workaround: Shutdown or remove the SVI.

- CSCtr65191

  QoS: Exp value is reset to zero when the class has Policer configured.

Ingress Marking does not work if packets are subjected to ingress marking and egress policer, the packet header is not modified according to ingress marking action configuration.

Workaround: None.

- CSCtr68091

  Convergence issue with multicast traffic, post route change.

  Workaround: None.

- CSCtr68870

  PowerTech: Debug Crash upon removal of SFP from SFP+ port.

  debug platform physical sfp can potentially crash the switch, if an SFP is plugged out of an SFP+ port.

  - 1G SFP is placed in a 10G SFP+ slot.
  - Console logging is enabled.
  - **debug platform phy sfp** command is invoked.
  - SFP in the SFP+ is plugged out.

  A crash may be seen within a few minutes.

  Workaround: Do not plug out an SFP, from an SFP+ port, if the command **debug platform physical sfp** is enabled.

- CSCtr70352

  Switch crashed after two days of longevity.

  Potential crash, if SNMP server is unreachable over a long duration of over two days, and SNMP traps are enabled.

  Conditions:

  SNMP traps are enabled in the switch, but the Management interface is either link down, or admin down, for a duration exceeding 48 hours.

  A crash may be seen a few minutes after unshut or admin up of the Management interface, while there is background activity by SNMP manager.

  Workaround: Ensure that management port link is up, if SNMP-Server traps are enabled on the switch.

- CSCtr71981

  Platform assert failures seen on deleting evc bd on port channel.

  When EVC bd along with l2tp feature is configured under port channel (with member added to the portchannel) and then it is removed from the port channel results in traceback from various place of code.

  Workaround: None.

- CSCtr74907

  Packets are incorrectly classified under COS/PREC instead of class-default.

  Classification is not working as expected in the case of some dynamic modification.

  Conditions: When defaulting an interface and adding back a policy in the presence of other policies in the system, classification does not work sometimes in egress.

  Workaround: Deleting and reattaching all policies in the system can fix the issue.

- CSCtr77082

  Improper bandwidth distribution on removing and adding classes in child policy.

  Bandwidth distribution does not work as expected during dynamic deletion/addition of classes.

  Conditions: When a class is deleted and added again and bandwidth is configured, bandwidth distribution does not work as expected.

  Workaround: Detach and reattach the policy to fix the issue.

- CSCtr32947

  Data path failing for 1K EVC xconnect between forwarding ASIC0-forwarding ASIC.

Resolved Caveats for Cisco IOS Release 15.1 (2) EY

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCtj18426

  With IGMP snooping forwarding does not happen for few entries.

  When there are snoop entries beyond hardware supported limits, the forwarding bandwidth drops for multicast traffic. However during testing, if the number of entries are within the hardware resource limits., (for the platforms, ME3800/ME3600), the aggregate bandwidth is acceptable.

  Workaround: Limit the number of snoop entries to be within the hardware supported limits.

- CSCtj83932

  Shaping counters are incorrect on Egress QoS policy.

  Cisco ME3600X shows higher shaping rate in "show policy-map interface" output instead of configured shaping rate. (the traffic received will be in accordance with the shape configured, issue is only with the counter display).

  Workaround: If the **show policy-map interface** command is issued with an interval of 3 mins (with load-interval of 30 sec on the interface), the counter display occurs as expected.

- CSCtn86291

  Traffic drop for >25 seconds on flex link switchover after preempt delay.

  Traffic drop seen for >25 seconds on flex-link port(s) upon switchover after **preempt delay <number> seconds** command is issued.

  In particular, this has been tested for a preemptive delay set to 3 seconds.

  Workaround: If not configured, the preemption delay is 35 seconds. And then the issue is not reported.

- CSCto55216

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

  When booting up Cisco ME 3600 switch, traffic going through the interface of the box may get dropped. The issue is intermittent, the packet loss lasts for several milliseconds.

  Workaround: None.

- CSCtq42860

  Packet getting leaked by the switch.

  The MPLS and OSPF packets received on the box's interface without any configuration seem to be sent over pseudowires configured on other interfaces.

  When an interface has no config, the OSPF and MPLS packets received on that are getting forwarded.

  Workaround: None. You must shut down the no config interface.

- CSCtr22554

  Error message appearing while giving shutdown/no shutdown on the interface.

  On shutdown/no shutdown on the interface where QoS policy is applied, error is seen. This error occurs only when the shutdown/no shutdown is initiated from a script.

  Workaround: None. There is no workaround for the script.

- CSCtr35554

  Traceback observed at ../src-nile/src-asic-nile/nile_adjmgr_l3m.c.

  When there is scaled config (of the order of 990 multicast entries) and the receivers connected to the box are removed, the following issue occurs:

  On a multicast setup with PIM SSM mode, the box throws the following traceback:

  ```
  *Jan 6 18:38:30.959 IST: platform assert failure: tbl_index < (NILE_MAX_VLAN +
  ADJ_MAX_PORTS + NILE_MAX_ETHER_CHANNELS): ../src-nile/src-asic-nile/nile_adjmgr_l3m.c:
  124: get_eaid_index
  *Jan 6 18:38:30.959 IST: -Traceback= 6900F4z 1DEEB40z 1F16E20z 1F17F48z 1F1AB24z
  2599184z 2C690E0z 2C6B9CCz 2C6D8B0z 2C6DF20z 2CCBB08z 2CC627Cz
  ```

- CSCtr53219

  Traceback observed@nile_adjmgr.c: 10612: del_l2m_phy_met.

  Tracebacks are seen when **show ip igmp snooping group vlan** command is used.

  Workaround: None.

- CSCtr53456

  ME3600 silent reload with SYS-2-BADSHARE error.

  Box reloads after the message below is displayed:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=D01B65C, count=0
  ```

  ME3600X went for silent reload, with 512 PWs configured and the traffic running over all the PWs. The setup was up and running for more than a week.

  Workaround: None.

- CSCtr58435

  Memory leaks @ IGMPSN L2MCM.

Memory leaks are observed at IGMPSN L2MCM process. This issue occurs when 200 vlan interfaces are added and then deleted using a script.

Workaround: None.

- CSCtr59079

  Platform assert failure on removing the OIF from multicast route table.

  Box throws the following traceback on removing an OIF from a multicast route:

```
        -Traceback= 618AF8z 1D79B94z 1E8AE9Cz 1E99A40z 1E9B3B4z 1E9B870z 250D678z
250DAD0z 250DBE4z 18CD3E8z 18EA1CCz 18DC9FCz 18B87D0z 251ABA8z 1F5A398z 1ABDE68z
platform assert failure: 0: ../src-nile/src-asic-nile/nile_adjmgr.c: 2420:
get_stored_efp_nile_id
```

  This traceback happens on a ten gigabit interface configured as routed efp which is connected to the receiver.

  Workaround: None.

- CSCtr61277

  Loopback message forwarding on port MEPs is broken

  Ping and Traceroute on CFM Port MEPs stop working after a certain period of time (around 2 days) on a back-to-back switch set-up. After a period of time, Ping and Traceroute started working again without intervention.

  Workaround: None.

- CSCtr61781

  Input policy traffic statistics get classified under Input policy-map applied on output policy.

  Statistics gets incremented for an incorrect class in a different policy-map. Only when traffic is reversed.

  When an input policy and an output policy are applied to incoming and outgoing interfaces, when the egress policy is removed and an input policy is attached to the egress interface, then traffic increments on the input policy of input interface when the traffic is reversed.

  Workaround: None.

- CSCtr61861

  Asserts and Tracebacks seen for adjmgr_l2_create_fwd_info.

```
platform assert failure: 0: ../src-nile/src-asic-nile/nile_adjmgr .c: 6412:
get_pw_di_adj Conditions:
```

  Workaround: None.

- CSCtr61989

  1K Scale EoMPLS: Crash observed @ nmpls_label_modify.

  When LDP is flapped continuously a crash occurs.

  Workaround: None.

- CSCtr66941

  entPhysicalChildIndex variable is not returning properly in ME3800 when the **getmany <IP> entPhysicalChildIndex** command is issued from the SNMP server.

  Workaround: None.

- CSCtr66974

  Platform assert failure: 0: ../src-nile/src-asic-nile/nile_adjmgr_l3m.c.

  Box throws the following traceback on doing an interface flap on the IIF interface multiple times:

```
*Jul 19 02:07:14.546: platform assert failure: 0:
../src-nile/src-asic-nile/nile_adjmgr_l3m.c: 1246: update_l3m_met
*Jul 19 02:07:14.546: -Traceback= 618AF8z 1D798F0z 1EA4150z 1EA4B8Cz 2525F0Cz 27E24FCz
27E6424z 27E7F24z 27E8588z 2846E6Cz 28415E0z
*Jul 19 02:07:22.578:     ##### vlan 8014 already exists in hdl 0x126709FC rpf_pass,
c_idx: 1, l_idx: 0
```

  Conditions:

  The IIF interface should be the only interface connected to the RP box. On doing repeated shut and no shut on this IIF interface, the traceback is seen.

  Workaround: None.

- CSCtr67113

  OSPF routes are lost on shut/no shut IRB EFPs.

  Switch does not learn routes again when the IRB efp is shut and then no shut.

  Workaround: None.

- CSCtr67291

  2 EVC's - Classification not working upon dynamic changes made on 1 EVC.

  CoS classification does not work when dynamic modification is done on input and output evc policies.

  This occurs when we have 2 cos policies per evc in input and output evcs. It has been observed that cos classification doesn’t work when we delete cos policy in input and output evc and add precedence based policies on input and output evcs.

  Workaround: None.

- CSCtr74374

  Traceback @ del_efp_met

  When EVC bridge domain is configured along with l2tp feature under more than one interfaces and then efp is either modified or removed traceback is observed. Traceback doesn't come if evc bd with l2pt feature is configured under only one interface.

  Workaround: None. Traceback is observed during deletion of evc but it doesn't affect the modification or deletion of the particular evc.

- CSCtr77213

  RPF-intf change leading to stale rpf programming @pd level.

  On doing RPF interface change, box does not program the RPF interface correctly for some entries. It still points to the older RPF interface.

  Workaround: Use the **clear ip mroute <group>** command to clear the affected group and RPF interface will get programmed correctly.

- CSCtr77238

  MFIB_PLTF-3-IOITEM_HANDLE_BAD:Space.0xE2252B8 -Process= "MFIB_mrib_read"

  Workaround: None.

- CSCtr77731

  REP keeps failing periodically on TE port.

  REP enabled TE port on ME3600 and ME 3800 goes to failed state without any trigger.

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

- CSCto07919

  System might reload due to malformed IPV6 packet.

- CSCtr63989

  L2PT forward broken over VPLS.

  Workaround: None.

- CSCtr69494

  Traffic is not flowing with the latest image with PIM SM.

- CSCtj50739

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

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

  Workaround:

  1. Do not change bridge-domain split-horizon group of an efp if there is a secured efp (mac sec enabled and restrict or protect violation mode enabled) in same bridge-domain.
  2. If split-horizon group of an efp needs to be changed, disable mac security of secured efps in same bridge-domain then change split-horizon group and re-enable mac security of secured efps.

Resolved Caveats for Cisco IOS Release 15.1 (2) EY1a

- CSCtj30238

  WRED counters are not updated correctly.

  WRED counters are updated incorrectly. The default counter should be 0, but the counter is incorrectly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.

  This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

  Workaround: Do not use WRED subclass Transmit packets/bytes counters.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtn89493

  Radius Packets are not honoured by the ACS server when Message Authenticator is included in the Radius packet where as when it is re-transmitted, it is honoured and ACS server is sending response.

- CSCtn38037

  attribute acct-session-id overloaded command causing malformed radius packets.

  gw-accounting aaa generate malformed radius accounting packets when **attribute acct-session-id overloaded** command is configured.

  Workaround: None.

- CSCtn16718

  Session is not established even after authentication passes. After failover happens with tacacs server, in the authentication stage even though authentication is passing, the session is not established. Load the UUT and NAS with the concerned image and establish PPP sessions between them.

  Workaround: None.

- CSCtn18784

  Increasing default bandwidth for Tunnel interface. Interface Tunnel 0 constantly sends high-bandwidth alarms.

  Workaround: None.

- CSCtk00181

  Password Aging when Crypto configuration fails. This is observed when Windows AD is set with **Password expires on next log on** command and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Authentication failure.

  Workaround: None.

- CSCtn12428

  Clear mpls counter not clearing VPN byte switched count **clear mpls counter** command does not work for vrf entries where outgoing interface associated is aggregate.

  When show mpls forwarding entry is VRF and outgoing interface is aggregate, the **clear counter** command does not clear the counter.

  Workaround: None.

- CSCto49918

  ping failed when l3vpn is configured non 0 gre key.

  When l3vpn profile is configured with a gre key, traffic over the tunnel is dropped. l3vpn configuration with a gre key is enough to reproduce the problem.

  Workaround: Do not configure a GRE key under l3vpn profile.

- CSCtq11526

  Embedded Packet Capture stops BFD neighbor adjacency.

  Enabling Embedded Packet Capture on the interface brings down the BFD neighbor relationship.

Workaround: None.

- CSCto82335

  Outstanding Access Transaction left unprocessed after Radius comes alive.

  Outstanding transaction Access transactions are 1. This test case is to check radius-server dead-criteria time 60 - It means within the 60 sec, the outstanding transaction has to process. In this case, outstanding transactions are 1.

  Please, check the above configurations. Initially radius-server interface is shut and created the session, and make the interface up and immediately clearing ppp sessions. It means, AAA doesn't have time to process the request.

  Workaround: Small delay is required between interface up and clear pppoe all and then check the **show aaa server private** output.

- CSCtr19922

  Potential crash executing **show adj internal dependents** command. Lots of output printed by **show adjacency** [*key of adj*] *internal dependents* followed by a crash.

  The symptom is observed with the existence of midchain adjacencies, which will be created by IP tunnels, MPLS TE tunnels, LISP, and similar tunneling technologies.

  Workaround: Do not use the **show adjacency** [*key of adj*] *internal dependents* command. Specifically, it is the **dependents** keyword which is the problem. If the **dependents** keyword is not used there is no problem.

- CSCtk17657

  Command **timeout 1** is unable to be reconfigured by rollback.

- CSCtr63114

  CDP disable resets management interface of ME3600.

  An ME3600 will reset the interface when disabling CDP (**no cdp enable**). If the interface is configuring with **no cdp enable** at bootup, the interface is down/down.

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

- CSCtl04112

  COA: 3750e crashes @ parse_coa_request.

  Switch/Router is reloaded whenever NAS receives State attribute in COA Request.

  While parsing COA Request, State attribute is decoded twice and original pointer was moved ahead and the next attribute type and length were wrong. So, it was looping and never exit.

  Workaround: As long as, State Attribute is not received in COA request, there is no issue.

- CSCtk98218

  Nasport values mismatch in start record pairs generated in same session when PRI interface is Used in NAS.

  Workaround: Use BRI interface in NAS.

- CSCtn63795

  A new cef entry added does not inherit all the forwarding attributes.

- CSCtr56977

  Multicast not working with "SVI+evc infra" access design.

When a single evc is configured on a Gig Trunk port, the svi (bdomain id) may not forward packets. This is seen intermittently and is usually seen when the interface modes are toggled between routed (L3) and (L2) modes (switchport trunk or access). The SVIs all come up fine but the forwarding may not occur.

Workaround: Shut/no shut the SVI interface and the traffic resumes. There is no drop seen due to this operation hence.

- CSCtq21258

  COA NACK'd when Radius pw larger then 32 bytes reduced to exactly 32 B.

  When a user uses a password larger than 32 bytes in size, the authentication for COA will pass if the password matches the settings on the RADIUS server. When this password is reduced in size to exactly 32 bytes, including the setting on the RADIUS server, the authentication for the COA will fail as the ISG appends excess data to the password sent to the RADIUS for authentication. This symptom is seen when the user password is larger then 32 bytes and is being reduced to exactly 32 bytes.

  Workaround: Do not use 32 bytes as the size for the user password. In case the error occurs, the only method to solve the issue is to reload the device.

- CSCtr31496

  Sip-200 LC crashes at hqf_sip1_work_with_callback after SSO with dmlpp.

  The line card crashes after switchover with the multilink configurations.

  Workaround: None.

- CSCts26757

  Image Suffix is missing for ME3800 images.

- CSCts31880

  PI PD entry not in sync/ S/W forwarding happens when src and rcv are removed.

- CSCtr72584

  On removal of CD from child policy, BRP assigned to CD doesn’t get cleaned.

  Removing and adding class-default to a HQOS policy-map does not work. On removing class default and reconfiguring class-default in a HQOS policy-map, validations and hence configuration fail.

  Workaround: Delete the policy-map and create a new one.

- CSCtq09376

  SIP200 crashed on multilink shut/noshut with QoS config.

  Customer observes continuous crash on SIP-200 after upgrading from 12.2-33SRD4 to IOS 15.1-2s. Service policy with priority command applied to Multilink interface.

  Workaround: Remove the service policy

- CSCts07998

  Continuous MAC flap after flapping forwarding ASIC1 core facing interface.

  VPLS traffic loops in a full mesh topology and MAC flap messages are continuously seen. This issue is seen if mac-address table is cleared causing unicast traffic to get flooded to the peer.

  Workaround: None.

- CSCtq16938

  IPv6 support on the switch.

- CSCtr83500

  OSPFV3 does not come up over switch acting as L2 switch. IPv6 Traffic is not passed when the box acts as a switch.

  Workaround: None.

- CSCtr89882

  NGMWR: Platform errors are seen in load balance scenario.

  Platform-related error messages are seen during an LDP flap in an ECM scenario.

  This symptom is observed with LDP with ECMP paths and during flapping of LDP sessions.

  Workaround: None.

- CSCtr83418

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

  Workaround: None.

- CSCtr87467

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

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

  Workaround: In order to get out of the situation a shut/no shut on Gig0 is necessary.

- CSCts06063

  Fix mplsD access issue when 3800 SDM template is used.

- CSCts40247

  SDM template update for switch.

- CSCts14910

  Multicast traffic doesn't converge fully when interface is defaulted and shut.

- CSCts49996

  IRB multicast support in fcs+1 rebuild throttle.

- CSCtr12104

  Qos: Support needed for police and set within the same class.

- CSCtr65191

  QoS: Exp value is reset to zero when the class has Policer configured. Ingress Marking doesn't work if packets are subjected through egress policers. When packets are subjected to ingress marking and egress policer, the packet header is not modified according to ingress marking action configuration.

  Workaround: None.

- CSCtr80397

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

  In certain conditions when running REP edge with no neighbor and **rep stcn stp** a TCN may not be sent to allow STP convergence on the neighbor. In a ring topology and having an ALT connection in the middle of the ring. And causing a failure next to that wasn't triggering a TCN to the STP neighbors to allow for mac convergence.

  Workaround: None.

- CSCts37959

  Traffic drop at egress interface configured with Priority+policer after reload.

- CSCts50039

  QoS: Support for vlan matches in port in the presence of EFPs.

- CSCts57152

  snmpwalk is not working for CISCO-CLASS-BASED-QOS-MIB in mcp_dev.

  CBQOS MIB values cannot be retrieved. When class based QoS is configured, the corresponding config / stats cannot be seen from the SNMP interface.

  Workaround: Use the command line to retrieve the values.

- CSCts57176

  Getting crash while loading the 15.1EY (v151_2_ey_rebuild_int).

- CSCts59569

  Marking does not work with Police+Set in the same class.

- CSCto64113

  Vc label allocation changes in case of RoutedPW on mcp_dev_nile.

- CSCts56018

  Issues found during IRB multicast UnitTest.

  This ddts was filed to take care of issues filed during UnitTest. The issues were found with IRB multicast configuration (multiple efp's as part BD).

  Workaround: None.

- CSCtr53056

  CRASH found @vlan interface while **no ip pim dense-mode** Command is configured.

  The Cisco ME3600 crashes due to watchdog timeout. This symptom occurs when switchport is configured on an interface that has PIM enabled. This is a timing issue and may not be seen every time.

  Workaround: None.

- CSCtq83601

  EoMPLS traffic stop after TE tunnel path change.

  EoMPLS traffic does not flow after MPLS TE tunnel path change after FRR. This symptom occurs under the following conditions:

  - The TE tunnel is used as PW.

  - The VC does not flap and label stack looks fine.

  This issue is seen only with port-based xconnect.

  Workaround: Shut/no shut the AC interface to try and resolve the problem.

- CSCtq39964

  IGMP query is not forwarded to spoke vc on H-VPLS.

  The igmp snooping is not forwarded to the spoke to core and core to spoke vc intermittently. The spoke/core where the packet is to be forwarded should come up later.

  Workaround: None.

- CSCtr03912

  MAC withdrawal is not working with REP ring.

  LDP Mac Withdrawal over VPLS with REP ring in the access is not working. When the access REP ring is broken it does not generate TC notifications causing MAC withdrawal to fail.

  Workaround: None.

- CSCtn07109

  n_pi1: IOSd/WCM crash with WCM sanity.

- CSCts60378

  Getting platform assert failure traceback continuously.

- CSCts03288

  ME3800 assert on boot up in nile_wrapper.c.

  Tracebacks in the router logs. Error in logs on boot up or configuration.

  Workaround: None.

- CSCts69328

  QOS: Mem-leaks during reload with VLAN grouping configurations.

  Memory leaks are seen after attachment of vlan grouping policy in the evcs on the interface. Attachment of any VLAN grouping policy in the presence of EVCs on the interface.

  Workaround: None.

- CSCts49505

  Porting IPv6 DDTS to v151_2_ey_throttle_nw.

- CSCts73357

  Memory leak @adjmgr_l3m_create_1st_eaid.

- CSCts76525

  Ingress exp marking not taking effect if we have egress marking with cos.

  Exp value is not set in the packet properly when egress cos marking is present in output policy. Packets which get ingress marked with exp and also get egress marked with cos, won't be marked with the ingress marked exp value.

  Workaround: Egress mark exp along with cos to set the topmost MPLS label exp value.

- CSCts47982

  Multicast forwarding rate goes down after config max-metric.

  Multicast forwarding rate decreased after max-metric was configured. ME3600x have 64SVI + 64PIM + 64 HSRP instance. Configure the max-metric on ME3600x, the multicast forwarding rate decreased.

  Workaround: None.

- CSCts60348

  L3 interfaces receive 2-times the traffic.

- CSCtq94357

  O/P of **show platform ip multicast groups 198.51.100.1 details**

show platform ip multicast groups 198.51.100.1 details does not throw the o/p based on the group address on licensed image, it throws the o/p for all groups in one go. Even terminal length is not working. But the same does not happen in switch-universal. It throws o/p filtered on group address which is queried for. The issue is seen only in the licensed image. It works fine in universal image.

Workaround: None.

- CSCts62981

  QoS: Tcams are utilized even though wred curve is rejected.

- CSCtr26677

  Router crashes at nrm_mplsd_get_hw_index after configuring MPLS core.

  Router crashes at nrm_mplsd_get_hw_index on running a script twice which configures **mpls ip** without reloading the box.

  Workaround: None.

- CSCts60931

  QoS: Packets are still marked even after deleting the class.

- CSCts60460

  Multicast traffic is not flowing with IRB config for all EFP.

- CSCtt00606

  EEM is broken in 15.1(2)EY.

- CSCts52604

  Router crash @ adjmgr_l3m_update_fid on sending joins o SVI interfaces.

- CSCtn20598

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

- CSCts15380

  Multicast traffic fails to flow unless ip igmp snooping/no ip igmp snooping.

  l2 multicast traffic failing to flow on reload with ip igmp snooping disabled for the vlan.

  Workaround: Enable ip igmp snooping and disabling the same.

- CSCts85655

  Tracebacks seen at MFIB_PLTF-3-ENTRY_LOCK with SM multicast test.

- CSCts63895

  S,G entry stuck in registering mode after reload.

- CSCts91603

  On switch rpf fail packets double accounted on qos policies of L3 ports.

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

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

- CSCtt01327

  No L2 ports are getting added to the L3 port list, with static igmp joins.

With static igmp joins and igmp snooping disabled multicast packets are not flooded on SVI. When igmp snooping is disabled after adding pim to svi.

Workaround: Reattach pim on the SVI.

- CSCto57632

  %COMMON_FIB-2-IFINDEXBOUNDS error messages on loading latest FCS+1 image.

  COMMON FIB IFINDEXBOUNDS error messages, on bootup or on clear counters. The messages would be noticed when we have PIM SM mode configured and have max supported multicast groups in use.

  Workaround: None.

- CSCtt16148

  Multicast Traffic received on wrong efp ports.

- CSCtr25386

  BFDv6 static route association fails after re-enabling interfaces.

  This symptom is observed after interfaces are re-enabled.

  Workaround: None.

- CSCts98245

  Switch crashed when configuring **ip multicast-routing**.

- CSCts34404

  CFM not working over flexlink.

  CFM does not work when configured over flexlink interface Cfm packets if received over standby flexlink interface, are also cataloged which leads to cfm config errors.

  Workaround: None.

- CSCtr82351

  ME3600 crash after ospf configuration.

  Router crashes when trying to change OSFP area/multipath parameters. NLFM learning process causes CPU HOG and the router is forced to crash by watchdog.

  Workaround: None.

- CSCtt24633

  Fix the build breakage caused by CSCts98245.

- CSCts62383

  ME38xx: Ethernet Linktrace fails with presence of MIP on ME38xx on switch.

  CFM linktrace message processing on switch fails to relay the packet when the to ‘be relayed port' or 'egress relay port' is a switchport. In all cased, cfm traceroute fails. Traceroute fails only when the egress relay port is a switchport.

  Workaround: None.

- CSCtr24751

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

  No special condition just peer BGP neighbor and ingress numbers of BGP route from TenGE.

  Workaround: None.

- CSCtr96774

  %PLATFORM_NCEF-3-ADJ: Traceback on configuring ip pim rp-address.

  Traceback seen on configuring ip pim rp-address.

  Workaround: None.

- CSCth02989

  When Copper SFPs are plugged in, forwarding ASIC LED process causes high CPU.

  High cpu-utilization on the device, and SFF8472 process goes to high cpu, when a large number of copper SFPs are plugged into a switch (ME3800x) device Only the **sh proc cpu sorted** command shows High CPU utilization (~45%) with SFF8472 process consuming the cycles.

  This is noticed ONLY when Copper SFPs are plugged onto the device. This caused by slow low-level access to the device.

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

- CSCtr53025

  ASF: Support for optics GLC-EX-SMD.

- CSCts45592

  Switch IPv6 neighbor goes to incomplete state approximately every 20 mins.

- CSCtt03126

  ME 3600X not passing Multicast traffic 224.0.0.x packets using EVC.

  ME 3600X not passing Multicast packets to 224.0.0.x through EVC configuration. Unicast traffic and multicast traffic except 224.0.0.x pass through without any issues. This has been observed on tengigabit interface on ME3600.

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

  Workaround:

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

- CSCts03228

  LTM and LBM packets not forwarded by remote after learning RMEPs.

  Ethernet cfm ping and traceroute does not work when the target Mep/Mip are on the me3600/me3800 device where the SVI/VPLS PW on the same service vlan has terminated.

  Workaround: None.

- CSCts27960

  Incorrect MAC Address Table Display for VPLS.

  The MAC Address-Table "Ports" display should appropriately print the peer end loopback id and vcid combination for addresses learnt on the pseudo-wire, instead of "VP". Every time a MAC address is learned on a pseudowire, the display is incorrect.

Workaround: None.

- CSCts68266

  mfib platform bad handle error messages.

  mfib platform error messages on joins after events like disabling/enabling ip multicast routing.

  Workaround: None.

- CSCtr79905

  Error msg while detaching and reattaching the policy on evc.

  Error message while detaching and reattaching the policy on evc interface when Port shaper is configured on the interface.

  Workaround: None.

- CSCtt01472

  Traffic gets dropped and resumes back with IRB configuration.

- CSCts02588

  Getting Trackback when changing RP on box.

- CSCtt37714

  Increase TCAM space for ACL for the Video template on ME3600.

- CSCts60971

  QoS: P-map getting detached on router reload because of tcam exhaust.

- CSCtt30722

  New number cannot be assigned to loopback IF on ME3600

  New number cannot be assigned to loopback IF on ME3600, even currently existing loopback Interface was deleted. If 64 numbers have been previously used and assigned to loopback interfaces.

  Workaround: None.

- CSCts94858

  L2 packets with different tags getting dropped with igmp snooping over PW.

- CSCtt39882

  QoS: Police in parent policy map and marking in child policy map is rejected.

- CSCtr58682

  Unable to configure **bridge-domain** CLI on the interface.

  Unable to configure bridge-domain under service instance. Seen only with the following sequence of steps:

  1. Configure service instance, encap, bd.
  2. Configure service-policy under the service instance and interface.
  3. Default the interface.
  4. Try to repeat step 1 again.

  We see that we are not able to configure the bridge-domain.

  Workaround: None.

- CSCtt28591

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

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

  Workaround: shut/no shut.

- CSCtt39886

  Ingress marking is lost when matching only the qos-group in egress.

- CSCtt20764

  SNMP traps not generated for ISIS related events.

  When configured **snmp-server enable traps isis** on the router, it is not showing up in **show run** configuration and also ISIS traps are not generated. This is seen with 15.1(2)EY release image.

  Workaround: None.

- CSCtr83330

  QoS: LDP Flaps on configuring HQoS policy-map on the core interface.

- CSCtt17741

  CPUHOG with second time deletion of vrf.

- CSCtr61408

  Found memory debug leak.

  Memory leak is observed for the memory allocated for MPLS VRF table. This is seen with basic configuration with or without l3 traffic. The leak is constant. This is seen when done through script.

  Workaround: None.

- CSCtt40847

  Traffic getting dropped on L3 interface, resumes on re-sending joins.

- CSCts79427

  Multicast traffic is not resuming after reload or disabling igmp snooping.

- CSCtt36429

  Multicast traffic punted to cpu.

- CSCtt41284

  Traffic gets dropped and resumes back.

- CSCts66394

  Traceback seen @ fib_assert_assertion_failed while booting the image.

  Upon boot the following error, together with an associated traceback can be generated:

  ```
  %COMMON_FIB-3-ASSERT: Assertion '_INTERNAL_ERROR_' failed in Common CEF []:
  Unexpected AF (non-fatal).
  ```

  This is a random occurrence at boot time, and to date has only been observed on a catalyst 3750. However, the cause is common to all platforms.

  Workaround: None.

- CSCto10254

  Router stuck at t/b -Process= "Collection process" on ospf shut.

- CSCtr17919

  Config shown in hex if **service compress-config** is enabled.

  When **service compress-config** command is enabled in the configuration, the **show startup-config** command will display a binary formatted file, similar to below.

```
#show startup-config
Using 874 out of 1572864 bytes00000000: 1F9D8C0A 420404C1 24CC1C3A 20C6BC71    ....
B..A $L.:  F<q
00000010:  6326CD99 3A72C2D0 49B33021 9A306ECE    c&M. :rBP I30! .0nN
00000020:  94012111 848C183A 64D4D051 E306882A    ..!. ...: dTPQ c..*
00000030:  54868098 52C70D08 2575D880 88615206    T... RG.. %uX. .aR.
```

  There is no impact to **show running-config** command, and Running Configuration is displayed in text format. If the user enables configuration compression, using the **service compress-config** command, followed by a **wr**. There is no impact to the Switch boot up configuration due to this.

  Workaround: If the user desires to view the startup-config on the Switch, the following steps can be followed.

  - In configuration mode, use **no service compress-config** command.
  - Commit the same, using **wr** keyword.
  - View the startup-config in the text mode.
  - If configuration compression is desired, again use the **service compress-config** command.
  - Commit the same using **wr** keyword.

- CSCts97872

  Getting platform assert failure traceback continuously.

- CSCtt33486

  With interface speeds of 10/100 the interface is not getting set to full-dup.

- CSCts63641

  EVC-xconnect shows incorrect EFP stats upon dynamic changes.

  EVC-xconnect shows incorrect EFP stats, when the EFP is deleted and reconfigured.

  Workaround: None.

- CSCtt98823

  Clock quality is not proper on 15.1(EY) image.

  Clock quality is bad when it comes from the switch. Normal network clock configurations are required.

  Workaround: None.

- CSCtt40711

  CLI for getting PVR/SVR values for PPC.

  Sometimes **show version** command does not show proper revision for PPC. It is inconsistent.

  Workaround: None.

- CSCts17548

  Chunk leak: NRM EMPLSINTD d & NMPLS backwalk.

- CSCtr86477

  gig0 starts down/down after bootup.

  Symptom 1: If CDP is disabled on the management interface of a Cisco ME3600 series switch, the port is down/down after bootup.

  Symptom 2: Regardless of CDP configuration, the management port is down/down after bootup.

  This symptom occurs under the following conditions:

  - Symptom 1 occurs only without the fix to CSCtr63114.
  - Symptom 2 occurs only with the fix to CSCtr63114.

  Workaround: Performing shut/no shut on the interface brings it back up/up.

- CSCtt42953

  SVI in VPLS stays down until attached to an interface even with AC.

  SVI with VFI staying down. SVI not attached to any trunk port, but has spoke vc attached to it.

  Workaround: Attach the SVI with VFI to a trunk port.

- CSCtu09389

  IGMP membership is not getting established.

- CSCtt01582

  SYS-3-CPUHOG and del_efp_met adjmgr_free_met on unconfig efp xconnect.

  Assert tracebacks were seen at del_efp_met when an existing config of 4000 BD having 4000 EFPs each was replaced with an empty configuration. Repeated configuration and unconfiguration of a scaled efp+bd config.

  Workaround: None.

- CSCtu20312

  PIM neighborship is not coming up over SVI based EOMPLS.

- CSCto56052

  MPLS Forwarding not working on PPPoA Dialer Interface.

  MPLS Forwarding is not working on PPPoA Dialer interface, when trying to ping a remote IP Address it shows the following error:

  ```
  %MPLS_PACKET-4-NOLFDSB: MPLS packet received on non MPLS enabled interface
  Virtual-Access2 L3 type 0x0281 label {16 0 1 254}
  ```

  MPLS is configured on both Dialer interface and Virtual-template, LDP comes up and shares the Label but Dataplane forwarding does not work.

  Workaround: Configure MPLS forwarding on GRE Tunnel, above the dialer interface.

- CSCtu21049

  Redundant code after collapse of rebuild_int to v151_2_ey_throttle_nw.

- CSCtu06627

  Traffic not forwarded to EFP when we leave from one grp and join 2nd grp.

- CSCtr40792

  Tunnel hwidb reused before free on standby.

  While configuring or using a TE Auto Tunnel the following tracebacks are seen every 60 seconds:

-Traceback= 6170E4z 2CE14D4z 2DD4210z 2DD50C0z 2CF4D34z 2FF79FCz 2FF35C0z 2F0095Cz 2F027ECz 2F02B30z 2F2C158z 2F48388z 2F49050z 2F495A8z 2F359A8z 2F35D14z

*Sep 19 17:34:29.221: %LSD-2-APP_NOTSUPP: Tunnel65437 interface does not support app TE Tun Intf

-Traceback= 6170E4z 2CE14D4z 2DD4210z 2DD50C0z 2CF4D34z 2FF79FCz 2FF35C0z 2F0095Cz 2F027ECz 2F02B30z 2F2C158z 2F48388z 2F49050z 2F495A8z 2F359A8z 2F35D14z

*Sep 19 17:34:59.221: %LSD-2-APP_NOTSUPP: Tunnel65437 interface does not support app TE Tun Intf

-Traceback= 6170E4z 2CE14D4z 2DD4210z 2DD50C0z 2CF4D34z 2FF79FCz 2FF35C0z 2F0095Cz 2F027ECz 2F02B30z 2F2C158z 2F48388z 2F49050z 2F495A8z 2F359A8z 2F35D14z

The hex output of the traceback varies depending on your code version with TE Auto Tunnels configured.

Workaround: None.

- CSCtr08841

  l2pt on evc xconnect enhancements.

- CSCto98835

  show ip igmp snooping groups vlan is not showing the IGMP V3 entries.

  Snooping on IGMP V3 does not work properly, this is an intermittent problem.

  Workaround: None.

- CSCtu21294

  IGMP snooping entry returns port list to be NullIdb.

- CSCts57295

  ME3600X with mac-address-table notification command crashed and reboot.

  The following commands are displayed by **show running configuration** command even if only **mac-address-table notification change mac-address-table notification mac-move** is used or only **mac address-table notification change mac address-table notification mac-move**. Also, you can delete all of them by deleting one pair of them.

  ```
  mac-address-table notification change
  mac-address-table notification mac-move

  mac address-table notification change
  mac address-table notification mac-move
  ```

  When reloading the device with the command above, the switch crashes and reboots itself all the time. Reload the device with the following commands:

  ```
  mac-address-table notification change
  mac-address-table notification mac-move

  mac address-table notification change
  mac address-table notification mac-move
  ```

  Workaround: None.

- CSCtr97166

  BPDUs dropped with EVC bridge domain and xconnect.

On ME3600X/ME3800X, BPDU's from customer interface are not forwarded when an xconnect is attached to a bridge-domain SVI. This affects both l2protocol forward and l2protocol tunnel configurations. For example:

Customer edge interface:

```
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan none
 switchport mode trunk
 service instance 100 ethernet
  encapsulation untagged , dot1q 1-4094
  l2protocol tunnel stp
  bridge-domain 100
!
interface Vlan100
 no ip address
 xconnect 192.168.1.1 100 encapsulation mpls
```

Note that normal L2/L3 traffic are forwarded as expected.

Workaround: None.

- CSCtu02164

  Rep fails periodically on TenGig port.

  REP enabled TE port on ME3600/ME3800 goes to failed state without any trigger. TE port on me3600/me3800 fails without any condition, just REP enabled. This is seen only when a 1000-Base SFP is used with the TenGig port. It is not seen with Gigabit interfaces.

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

- CSCto60808

  Crash at atmoc3pom_preprocess_tx_pak when traffic is started.

  Device can reload when QoS is enabled and traffic load activates QoS. Hierarchical Queueing Framework (HQF) is used on ATM.

  Workaround: None.

- CSCtu09542

  Platform Assert failure messages continuously with Scale test cases.

  Tracebacks seen with scaled IRB multicast configs. Seen only with scaled IRB multicast configs. When you add/delete oifs from multicast group.

  Workaround: None.

- CSCts10366

  Write Core via FTP causes system crash.

  Have configurations to enable core write to FTP server.

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

  The command **write core** will cause a system crash.

  Workaround: None.

- CSCtt21887

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

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

  Workaround: None.

- CSCtt71261

  Met is not programmed correctly for the OIF/ DestIndex is incorrect.

  This is seen when you reload the box with IRB multicast configurations. It is seen only during bootup. Second eaid and CQE's are not created in this case resulting in the wrong met index being used.

  Workaround: Remove and add "ip pim" from vlan which has efp's.

- CSCtu31659

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

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

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

- CSCts79107

  Switch blocks DHCP packets with broadcast flag.

  DHCP packets with broadcast flag is blocking by the switch.

  1. switch ME-3600X-24FS-M
  2. configured DHCP relay
  3. **switchport block multicast** command in config

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

- CSCts08628

  ME3600x 10G ports multicast storm-control is broken.

  10G ports multicast storm-control isn't working.

  Workaround: None.

- CSCts37316

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

  When an IOS file is downloaded prior to version up, the utilization of CPU become 100%. This situation lasts about 8-9 minutes.

  Workaround: None.

- CSCts08326

  Claim support for CISCO-CLASS-BASED-QOS-MIB.

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

  Workaround: None.

- CSCts80581

  Need a syslog warning message if TCAM for Unicast routes gets exceeded.

- CSCtt95945

  Traffic gets dropped with scaled IRB config/Met chain is incorrect.

  The issue is seen when you have multiple svi oif's with efps under them and when you add/delete new oifs.

  Workaround: clear ip mroute *

- CSCto72927

  MF: Registering a TCL policy causes cat4k to hang.

  Configuring an event manager policy may cause a cat4k to hang. Configuring a TCL policy and copying that policy to the device.

  Workaround: None.

- CSCtu24685

  nile_tcam_add_entry_mask Error Messages on 3600.

  nile_tcam_add_entry_mask error messages are thrown, scaled config of EVC XConnect.

  Workaround: None.

- CSCtg48785

  sh x25 hunt-group causes %DATACORRUPTION-1-DATAINCONSISTENCY: copy error.

  The following error may appear in the log:

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

  This issue occurs while issuing show x25 hunt-group command when a large amount of x25 traffic needs to traverse the device.

  Workaround: Do not use the show x25 hunt-group command.

- CSCtt99101

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

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

  Workaround: Reload the box.

- CSCtu33389

  SyncE Issue when unplugging the cable connected through BITS port.

  When we unplug the cable connected through BITS port which is in 2048k framing mode, we are not detecting signal failure for BITS.

  Unplug the BITS cable or shutdown the BITS port.

  Workaround: None.

- CSCts71780

  IPv6: IPv6 traffic gets punted with MPLS core.

  IPv6 traffic coming on the interface was getting punted to CPU, when the IPv6 interface has IPv4 configured under a VRF. IPv6 and IPv4 configured under the same interface with IPv4 under the VRF routing.

  Workaround: None.

- CSCtu53852

  MST broken with fix of CSCtr97166.

  MST packet broken over EVC-BD.

  Workaround: None.

- CSCtt94445

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

  no class class-default

  Workaround:

  1. Delete re-configure policy-map again.
  2. Delete and re-configure "police cir xxxxxx" again.

- CSCtu19557

  ME3800: Domain option is not available while configuring CFM/ELMI interwork.

  While configuring CFM/ELMI interworking (CFMoXconnect or CFMoEVCBD), the domain option is not available while configuring interworking. Without this, CFM/ELMI interworking is broken for CFMoXconnect.

  Workaround: None.

- CSCtu32445

  SNMPv3 polling failed on ME3800.

  using auth-priv

  Workaround: Use AES instead.

- CSCtu28820

  Traceback seen upon sending IGMP leave for more than 150 groups.

- CSCtu21202

  IGMP leave message not sent over PW when IGMP sn is enabled.

- CSCtr72021

  L2 traceroute does not work on EFPs and MAC on vlan 0

  Workaround: None.

- CSCtu93151

  Intermediate mac addresses learned does not age out.

  Dynamically learned mac address does not get aged out. Without traffic mac address continues to persist in mac table.

  Workaround: Clear mac address table using cli **clear mac-address-table dynamic**.

- CSCtt08818

  ME3800: IP SLA Ethernet jitter probes do not work.

  IP SLA jitter does not work. **ip sla statistics** command displays proper jitter information.

  Workaround: None.

- CSCts17336

  L2PT becomes inoperable upon toggling bd or encapsulation configs on an EVC-BD.

l2pt does not work when encapsulation or bridge domain value is modified under efp. No l2 protocol pdus can be tunneled or forwarded.

Workaround: None.

- CSCtt01353

  Traffic flooded on non-rpf interface in case of RPF fail.

- CSCts69425

  Traffic is not flowing with L2 Port-channel, working fine with L3 Port-channel.

- CSCtw41796

  Multicast traffic looped back on the same port it was received from.

  Multicast Traffic loops back to same interface from which it is coming. The shut-no shut on mrouter having EFPs.

  Workaround: Disable and enable igmp snooping or unconfig and reconfig the efp.

- CSCtu18361

  Switch stops forwarding after flapping VPLS vc.

- CSCtu42288

  The "nile_tcam_add_entry_mask" messages are flooded in the console.

  Tracebacks seen on loading an image with video template on me3600. This is seen on bootup.

  Workaround: None.

- CSCtu35217

  SDM template sometimes changes to default template.

- CSCtu31420

  ARP resolution fails with routed BD.

  ARP failure. Trying to resolve arp via routed BD.

  Workaround: clear mac address for the bridge-domain on which ARP is being resolved.

- CSCtu21310

  Tracebacks at MFIB_PLTF-3-ENTRY_UNLOCK_FAIL on unconfiguring PIM.

- CSCtu24263

  Observing traceback on mrouter upon shutting down the interface.

- CSCtu23538

  Multicast traffic drops and resumes on its own.

- CSCtu22952

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

  A Cisco ME3800 may stop forwarding traffic suddenly when the port channel has EVC configuration.

  The problem happens when Port-channel interface with multiple member link on LACP is configured via EVC. By sending single Source-Destination traffic, it was seen to be moving from one member link to another.

  Workaround:

  – Use etherchannel instead of LACP.

  - Remove EVC.

- CSCtu20763

  Traffic gets doubled on clearing ip mroute on source box.

- CSCtu31962

  Chunk bad magic errors on making TE tunnels to choose diff path option.

- CSCtw33503

  Cisco-flash-mib needs to be supported on switch-15.1.2.EY train.

  NCCM functionality is not working.

  cisco-flash-mib needs to be supported.

  Workaround: None.

- CSCtw42189

  BIT-OUTOFRANGE Errors on flapping MST with traffic.

- CSCtw50053

  IFM on efp xconnect does not work with mpls explicit null. IFM on efp xconnect does not work with mpls explicit null in the mpls config.

  Workaround: None.

- CSCtu35933

  L2 Multicast stop flowing for some groups over EVC with IGMP snooping. L2 Multicast groups stops being forwarded across EVC with IGMP snooping enabled. This occurs where there is a lot of igmp activity and happens after a long time.

  Workaround: None.

- CSCtr74907

  Packets get classified incorrectly under COS/PREC instead of class-default. Classification is not working as expected in the case of some dynamic modification. Having detached and reattached a policy which matches on dscp/prec, dscp based classification doesn't work as expected. The issue occurred because dscp qos-label wasn't getting cleared when a policy was detached from the trust table.

  Workaround: Deleting and reattaching all policies in the system can fix this issue.

- CSCtu36333

  ME36xx console not working at speed 300. Baud Rate of less than 1200 is not supported on ME36xx platform. Supported baud rate range 1200 - 115200, default baud rate is 9600.

  Workaround: None.

- CSCtt30509

  Able to guarantee more bandwidth on child greater than parent shaper on EVCs. Guarantee more than available bandwidth at leaf level classes. This is not logically possible, but the configuration allows the same. HQoS with shaper in parent and absolute bandwidth in child. Sum of child bandwidths is greater than parent shaper.

  Workaround: When configuring a HQoS policy-map, make sure the sum of bandwidths on child classes is less than the parent shaper.

- CSCtw54959

  Port does not leave group after sending leave, with ONLY static mrouter port. IGMP groups are not removed when leaves are received and there is only static mrouter ports and immediate leave is not configured.

  Workaround: None.

- CSCtw56522

  IRB Multicast - support 64 oif per (S,G), where there are multiple efps configured per bridge domain.

  Workaround: None.

- CSCtu38228

  ME3600 crashes when the core interface is shut. Me3800 crashes when core interface flaps and with svi PWs passing traffic.

  Workaround: None.

- CSCtw59163

  L2PT tunnel on EFP xconnect not working. L2pt tunnel on Efp xconnect isn't stable. May not work at times. Triggers include link flaps, PW flaps and other dynamic events.

  Workaround: None.

- CSCtw66179

  Correction for igmp snooping by broadcast loop fix.

  Workaround: None.

- CSCtw60774

  Single broadcast traffic is replicated to large value on SVI EoMPLS. MAC Flap notification will be seen on the PE device where SVI EoMPLS is configured and there will be decreased throughput. Broadcast or ARP request sent are sent back on the PW from where it came.

  Workaround: If the requirement is to send traffic from a particular customer to another customer, then EFP xconnect can be used as a workaround.

- CSCtw48499

  H-VPLS: End-to-End Device Ping does not flow over VPLS VCs. End-to-End ARP resolution/l3 ping failure of vpls/svi based eompls. This issue occurs when there are more than 3 EFPs and pseudowire (xconnect) in same bridge-domain on any of the PE devices.

  Workaround: Configure the EFPs first and then configure the pseudowire (xconnect) under the SVI.

- CSCtt15870

  ME3800: CFM Remote port state shows UP instead of Blocked. On ME3800/Me3600 CFM Remote meps on evc bridge domain, port state shows UP instead of Blocked. Evc states are not correctly shown.

  Workaround: None.

Resolved Caveats for Cisco IOS Release 15.1 (2) EY2

- CSCto46716

  TE tunnel is not added into RIB even when it is found in forwarding-ad and OSPF

Routes over the MPLS TE tunnel are not present in the routing table.

This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In **debug ip ospf spf**, when the SPF process link for the TE tunnel is in its own RTR LSA, the Add path fails: no output interface message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto31265

  OSPFv3: ABR does not translate Type7 when primary Type7 is deleted.

  ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available. This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/re-add the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCtn65974

  Tacacs+ command authorization failure not respected by router.

  When an unauthorized user tries to set an ext-community in a route-map, the router gives a Command authorization failed. message as expected. In the end the parser does accept the set ext-community command however as it can be seen in the configuration afterward.

  Most route-map set and match commands exhibit this behavior.

  - This is seen in 12.2(33) SRD and SRE IOS images.

  - Router is configured for tacacs command authorization.

  - Tacacs server is configured to deny the **set ext-community** command for the user.

  Workaround: None.

- CSCtn97451

  BGP peer router crashes after **clear bgp ipv4 unicast <peer>**.

  Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router. This symptom occurs with the following conditions:

```
Router3 ---ebgp--- Router1 ---ibgp---  Router2

ROUTER1:
--------
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
!

router ospf 100
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.3 remote-as 11
!
```

```
ROUTER2:
--------
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 100
 redistribute static
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

ROUTER3:
-------
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip pim sparse-mode
!

router bgp 11
bgp log-neighbor-changes
 network 0.0.0.0
 network 0.0.0.0 mask 255.255.255.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. **clear bgp ipv4 unicast 10.1.1.1** on ROUTER2.

Workaround: None.

- CSCtn38225

  Route-Server show commands missing header info.

- CSCto31639

  BGP dynamic neighbor does not work on VRF.

  BGP Dynamic neighbor feature VRF-aware support. The support was not present before this fix.

  Workaround: None.

- CSCto35280

  ASR1K route reflector issues with prefix-length-size knob for interop.

  Peer-group or template configuration overrides, locally configured pref-length-size for the peer.

  1. prefix-length-size is locally configured for the peer.
  2. Peer is configured under peer-group or template and activated under afi L2VPN.
  3. Knob is configured differently for the peer-group or template, as compared to the peer.

  Workaround: None.

- CSCto88581

  Standby crash in nsr interface message checkpoint handler.

  The standby RP crashes following an interface configuration change. This symptom is observed only when **ospf non-stop routing** command is configured.

  Workaround: None.

- CSCto66178

  BGP can prematurely send EOR to peer in a particular case.

  When there is continuous route churn, BGP can send EOR as refresh is done for the peer. The EOR should be done only when both refresh/modified routes are sent.

  Workaround: None.

- CSCtl81217

  Loosing rip config on interface after a reload Cisco ME-3400G.

  Customer has **ip address dhcp** command and rip configured on one of the interface:

```
interface GigabitEthernet0/1
port-type nni
no switchport
 ip address dhcp
 description Port physique face au reseau
 ip rip authentication mode md5
 ip rip authentication key-chain keys_ripv2_md5
```

  After reload of the box, following 2 lines are lost on the interface:

```
 ip rip authentication mode md5
 ip rip authentication key-chain keys_ripv2_md5
```

  This behavior is only seen when **ip address dhcp** command is configured on interface. If static IP address is assigned to interface, this issue is not seen.

  So main concern is that even after an IP address is assigned using DHCP, the rip config is not applied back on the interface.

  Workaround: None. EEM script can be used to add commands on interface after IP address is assigned using DHCP.

- CSCto41165

  Line-by-Line sync failure for **ip extcommunity-list 50 permit**.

  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit|deny** command, and then the **no ip extcommunity-list 55 permit|deny** command. This symptom occurs when the standby router is configured.

  Workaround: None.

- CSCtl01141

  SNMP: cswmMvrfStatsTable not populated in CISCO-SWITCH-MULTICAST-MIB.

  cswmMvrfStatsTable does not get populated. This symptom occurs when the multicast vrf instance is configured on any switch running mtrose image and mibwalk is configured on cswmMvrfStatsTable.

  Workaround: None.

- CSCto42998

  InQ buildup post-switchover at new active RP.

- CSCto69062

  show bgp ipv4 unicast summ displays incorrect dynamic bgp peer count.

  Inconsistent dynamic neighbor counter is summary commands when dynamic neighbors are configured with multiple afis.

  Workaround: None.

- CSCtj21226

  New best path fails to be preempt existing best on withdraw.

- CSCtl51857

  Router crashes at bgp_session2topo_cap_base when changing rs context.

  The route-server might crash due to a rare timing situation when the route-server context is deleted or changed for an RS peer. This might happen when the RS is servicing a refresh or sending updates during the convergence. In a rare event of changing or deleting the route server context on a peer can lead to a crash. This occurs when the change is made while the router is converging or servicing a route churn.

  Workaround: Do not delete or change the route-server context when there is a large scale refresh or update going on towards the route-server client peers.

- CSCtn68117

  Win11: Session command does Not work on Cat2975.

  Session command does not work on Cisco C3K series routers that have become the master after a mastership change. This symptom is seen when fail-over to slave occurs.

  Workaround: None.

- CSCtn95340

  Route-map not pre-pending Confed routes when **continue** option is used.

  Route-map not pre-pending Confed routes when **continue** option is used.

  Topology:

  ---------- RT-A ----------RT-B----------RT-C

  in the above topology, we have three routers RT-A, RT-B and RT-C. where RT-A and RT-B are sharing confed AS (16096). and RT-C is the normal eBGP to RT-A.

  Now if RT-B tries to configure the route-map with continue option to pre-pend the AS-path to the routes learned from RT-A, and advertises it to RT-C. These routes are not pre-pended with the mentioned as-path in the route-map.

  Workaround: None.

- CSCto00796

  BGP stops advertising RT extended community to peers in a peer-group.

  In a rare and still un-reproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR). This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE (+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- CSCto72629

  OSPFv3 Neighbor Down: Too many retransmits repeatedly after peer SSO.

Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless max aging is initiated by OSPFv3 process.

Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto99523

  Slow BGP convergence with High CPU consumed by BGP Router on PE ASR RP2.

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq18459

  CLI errors for **bgp confederation peer** *as-number ...*

  If you enter **bgp confed peer** command is taken. On an HA system, if you then type **no bgp confed peer**, you may cause standby to reload. If you enter **bgp confed peer 1 2 3 xyzfsasdf any-text**, you'll get unrecognized command, but the effect is shown in **show run**: **bgp confed peer 1 2 3**.

  Typing in command syntax that is technically allowed, but semantically wrong.

  Workaround: Avoid making such manual mistakes.

- CSCtq04117

  VPN traffic is dropped after the SSO at the remote end.

  DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running. This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
  2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

  Workaround: Use the **clear ip route vrf x** command.

- CSCtf40858

  % Prefix-list filter exists, de-config first error when no such filter.

  The **distribute-list** command with ACL or route-map filters cannot be configured.

  After a distribute-list with a prefix list filter via the interface with OUT filtering direction is configured and removed, the distribute-list with ACL filter via the same interface with OUT cannot be configured.

  Workaround: No workaround except erasing/enabling the router instance.

- CSCtk97033

  SYSFLAG_CONFIGURED notification missing in component.

- CSCtw51585

  Device crashed with scaled config and executing **show ip igmp snooping**.

The device goes into a hung state or subsequently is brought down due to simultaneous display of show commands and receipt of leaves at the same node.

This is a very rare occurrence wherein leaves for all the groups joined come at the same instant and during the same time, the box is occupied in displaying all the groups by issuing a show command and forcing terminal length to 0.

Workaround: Set terminal length to some non-zero value.

- CSCtw75076

  ME3600: A few packets get duplicated in sparse mode deployment.

  Duplicate multicast packets are seen in pim sparse-mode.

  Workaround: None.

- CSCtw80099

  ME3600 QoS: P-map is rejected if it has police+priority and bandwidth.

  Policy-map with police+priority and bandwidth is rejected. This happens when police+ priority and bandwidth is configured in the same policy map.

  Workaround: None.

- CSCtw85509

  ME3600 show process xxx are Ambiguous command in **show tech**.

  The problem is that the following command's log is not in **show tech**.

  show process memory

  show process cpu

  show process cpu history

  If you enter **show process xxx** only, the command is showed the following:

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

  This occurs on ME-3600X-24FS-M switch running Cisco IOS Release 15.1(2)EY1.

  Workaround: Use the following commands:

  show processes memory

  show processes cpu

  show processes cpu history

- CSCtu21330

  Assert failures at adjmgr_free_met on configuring SVI based EoMPLS.

  Assert failures are seen while unconfiguring PIM from SVI. PIM running on SVI & IGMP joins sent to this mrouter.

  Workaround: None.

- CSCtw74099

  ME3600X crashes with ttl macro and SNMP access.

  ME3600 may crash if the etsec tx ring hangs. This occurs if the management port is up and etsec tx ring hangs.

  Workaround: Shut down the management port.

- CSCtt31368

  ME3600 wrong optical alarm Thresholds for CWDM SFPs.

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

  Workaround: None.

- CSCtw53043

  QoS: Policer configuration has exceeded hardware limitation.

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

  This occurs on the ME-3800X-24FS-M switch running, me3800x-universalk9-mz.122-52.EY2.bin.

  However, the configuration has not reached the 4096 policers that are configured on the switch.

  Workaround: None.

- CSCtu14878

  ME3800: ECMP Causes VPNv4 traffic blackholing.

  In unknown circumstances, when ECMP paths are created between an ME3800 vpnv4 Pre-Agg router and an ASR9000 3107 ABR router (through HA failures or intentional configuration) the ME3800 will blackhole all VPNv4 traffic. This occurs under the following conditions:

  - Running IGP to 3107 ABR router
  - Running labeled BGP to reach far end destination and to provide VPN labels
  - Have ECMP paths from ME3800 to ASR9000 ABR router as shown from **show ip cef vrf vrfname prefix mask det**

  Workaround: None.

- CSCtw50289

  ME3600: forwarding ASIC labeled BGP scale restricted to 8k.

  The ME3600X/ME3800X cannot scale more than 8k ibgp+label scale, with current implementation of egress label storing.

  Workaround: None. Need Egress label storing algorithm enhancement, so that the switch can scale more than 8k.

- CSCtw86851

  EVC shaper does not affect SSM mcast traffic or breaks it when removed.

  When service policy is applied on evc and this evc part of svi with l3 multicast enabled. The issue is seen only with multicast traffic.

  Workaround: remove/add **ip pim sparse-dense-mode** from svi interface.

- CSCtw79815

  Mem leak at nile_qm_alloc_eqos_vmr_entry during router bootup.

  Memory leaks observed after bootup. Memory leaks observed at nile_qm_alloc_eqos_vmr_entry.

Workaround: None.

- CSCtw80393

  ME3600X: QinQ L2 unicast forwarding not programmed correctly.

  QinQ packets dropped on ingress switchport trunk. Egress port should be EVC, packets should traverse through the switch twice and MST convergence should occur.

  Workaround: **clear mac address table**

- CSCtu02455

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

  Egress QoS service-policy does not classify 'marked' packet correctly when applied to Layer 3 port channel members. The issue is seen only when the port channel is layer 3. The issue is seen in Cisco IOS release 12.2(52)EY and 15.1(2)EY.

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

  OR

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

- CSCtw77884

  L2PT: STP not being tunnelled with EVC xconnect.

  MSTP bpdu's are not tunneled with l2protocol tunnel command. This has been observe in 15.1(2)EY1a with following configuration:

```
interface GigabitEthernet0/1
service instance 501 ethernet
  encapsulation untagged
  l2protocol tunnel cdp stp
```

  Workaround: Use l2protocol forward.

- CSCts39284

  Bottom of label stack not set when ibgp+label (RFC 3107) is configured.

  Packet corrupted, because the bottom of label stack bit is not set correctly when ibgp+label is configured.

  Workaround: None.

- CSCtx05464

  CE Multicast fails over full mesh VPLS.

  CE multicast fails over VPLS when the PE device is a ME3800x. This occurs when VPLS is configured in a mesh with at least 5 VPLS peers.

  Workaround: For routing protocols, use **unicast neighbors**

- CSCtw79488

  Multicast is not forwarded to AC with xconnect under SVI without IP.

  Multicast is not forwarded out on EVC. This has been observed in Cisco IOS Release 15.1(2)EY and 15.1(2)EY1a in the following configuration:

```
interface GigabitEthernetx/y
 switchport trunk allowed vlan none
 switchport mode trunk

 service instance <> ethernet
  encapsulation dot1q <VLAN-1>
```

```
  l2protocol tunnel
  bridge-domain <BD>
 !
!

!
interface Vlan<BD>
 no ip address
 xconnect <IP> <VC-ID> encapsulation mpls
!
```

Workaround: Configure any dummy IP address on interface Vlan. It does not need to be in the same segment.

```
!
interface Vlan<BD>
 ip address A.B.C.D M.M.M.M
 xconnect <IP> <VC-ID> encapsulation mpls
!
```

- CSCtu02405

  Egress policy-map counters not accurate on ME3800x.

  Stats are incorrect at the interface level for port-shaper. Fixed the statistics update.

  Workaround: Refer to the EVC statistics which are updated correctly.

- CSCtx24671

  Nested crash observed on defaulting interface.

  Workaround: None.

- CSCtw97513

  ME3600/ME3800: L2PT: STP BPDUs are not sent over the VPLS PW.

  STP BPDUs not sent over more than one vfi neighbor. This occurs with full mesh VPLS, STP does not converge end-to-end.

  Workaround: None.

- CSCtx28468

  ME-3800x crashes with specific ARP packet.

- CSCtx36100

  Observing Crash@pm_platform_get_gid_from_idb with Latest XE36.

  Crash upon unconfiguring static MAC address entry. When the static MAC address is associated with multiple interfaces.

  Workaround: None.

- CSCtx05882

  QL values are not proper on BITS interface.

  Workaround: None.

- CSCtw94048

  Interface is selected by clock selection algo. even if it is in up/down state.

  Workaround: None.

- CSCtw61035

  PM-4-BAD_COOKIE SM-4-BADEVENT seen on interface up/down.

  Interface up/down triggers these messages.

  Workaround: None.

- CSCtx20680

  EVC BD Traffic does not resume after removing and adding Service Instance.

  Workaround: None.

- CSCtx42722

  Routed multicast traffic not forwarded out all interfaces in OIL on 15.1.

  Routed multicast traffic not forwarded out on all interfaces in OIL. This issue is seen in Cisco IOS Release 15.1EY.

  Issue can be verified by checking **show plat ip multicast group** [*group*] **detail**. If the issue is encountered, ports will be missing from the OIF for the S,G entry:

```
Switch# sh platform ip multicast groups 224.0.10.135 detail
GROUP_ADDR 224.0.10.135

NMDB (*, 224.0.10.135) nmdb->0xD7E82E4, entry->0xE53D134 magic 0x9E tcam hdl:0x277
nh_rpf_p:0xC3D85F8 nh_rpf_f:0xC3D8498 fid_hdl:0x13FD4D3C(idx=0xBEB1) rpf pass:cpuQ:4
rpf failed cpuQ:5
 flags: HW, pflags: SPT,

RPF INTERFACE-> intf 501 port count (1) p10

RPF pass OIF interface count 1 hw_cnt 1
intf 224 port count 1 flags=0x8
 p11 <<<--- Correct port information getting reflected

RPF failed OIF interface count 1 hw_cnt 1 intf 224 port count 1 flags=0x8
 p11

GROUP_ADDR 224.0.10.135

NMDB (10.0.2.70, 224.0.10.135) nmdb->0xD7E64B4, entry->0xE53A494 magic 0xB6 tcam
hdl:0x298 nh_rpf_p:0xC3DE4D8 nh_rpf_f:0x0 fid_hdl:0x13FDF8CC(idx=0xBEED) rpf
pass:cpuQ:0 rpf failed cpuQ:6
 flags: HW, pflags:

RPF INTERFACE-> intf 501 port count (1) p10

RPF pass OIF interface count 1 hw_cnt 1
intf 224 port count 0 flags=0x8
                              <<<<<---- Missing port information
```

  Workaround: Issue **clear ip mroute** [*group*] for the group in the broken state.

- CSCtx04826

  Alarms on BITS are not reported to netsycn algo.

  Workaround: None.

- CSCtw57473

  Traceroute mpls traffic-eng and ping mpls traffic-eng cmd are missing.

  Traceroute **mpls traffic-eng** command and **ping mpls traffic-eng** command are missing in ME3600x.

Workaround: None.

- CSCtw93630

  ME3800: CFM CC message stops cataloging after cfg/uncfg QOS policy.

  CFM CC message stops cataloging after configuring QOS policy. When CFM is enabled globally, if we attach an input service-policy followed by an output service-policy, then CFM CC messages stop flowing.

  Workaround: None. Detach the qos-policies and reload the box.

- CSCtw83135

  Router crashes on clearing igmp group on PW on peerover SVI based EoMPLS.

  Router crashes on clearing igmp group over SVI EoMPLS.

  Workaround: None.

- CSCtx45131

  ME3800 locks to a bad quality clocks but with good advertised QL.

  A Metro Ethernet Switch ME3800 may lock on a poor quality clock via SyncE. This problem is observed when the received clock is advertised with a good quality via ESMC.

  Workaround: None.

- CSCtq29157

  BYTES SYSTEMS: interface throughput is low when changing the configurations.

  Workaround: None.

- CSCtx18897

  Traffic forwarding issue after link flaps with MPLS-TE/FRR.

  Workaround: None.

- CSCtx51815

  Traffic forwarding issue with xconnect over MPLS-TE/FRR.

  Workaround: None.

- CSCtw97578

  W2:IO MODE2 (8+4):SYS-2-CHUNKBOUNDSIB observed while flapping core links.

  CHUNKBOUNDSIB error message. Flapping mpls core links.

  Workaround: None.

- CSCtw88330

  CPU-HOG is seen with synchronous mode on port-channel interface.

  Workaround: None.

- CSCtu72323

  Add show logging in **show tech** for ME3600 and ME3800.

  This bug requests that **show logging** command be shown in show tech-support for ME3600 and ME3800.

  Workaround: None.

- CSCtr71981

  Platform assert failures seen on deleting evc bd on port channel.

Workaround: None.

- CSCtx42616

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

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

  Workaround: None.

- CSCtx76174

  REP goes down with 'vlan dot1q tag native' command.

  Rep between me3600 and me3400 or any other switch could fail.

  This is seen only when the other switch has **vlan dot1q tag native** command configured.

  Workaround: Enabling **debug platform cpu-queue stp** on the me3600 recovers rep from failed state. Other work around would be to disable **vlan dot1q tag native** on the connected device.

- CSCtw69431

  Traceback seen with "%SYS-3-INVMEMINT: Invalid memory action (malloc)."

  If a ME3600X configured with **ethernet oam** on an interface that is up loses power, it will generate an SYS-3-INVMEMINT and a Traceback. Power is lost to the switch.

  Workaround: None.

- CSCtx62215

  Ingress marking stops working after a reload.

  In the presence of ingress and egress marking, ingress exp marking is not effected in packet. This issue is seen only when we reload the box in the presence of ingress and egress marking.

  Workaround: Detach and reattach the ingress policy which does exp marking.

- CSCtx65533

  GLC-FE-100FX duplex setting is not nvgened.

  Workaround: None.

- CSCtx79802

  Network clock input source cli is accepted for non supported interfaces.

  Workaround: None.

- CSCtx82223

  QoS: Incorrect classification on member-link Pmap on router reload.

  On router reload the classification is not working correctly on qos applied on the member-links. This issue occurs when you reload the box.

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

- CSCtx45831

  W2: mcast traffic does not flow through Port-channel.

  Workaround: None.

- CSCtw85629

  Switch gets hung when ssm option is changed on the peer.

  Workaround: None.

- CSCtx18366

  Switch gets hung when ssm option is changed on the peer.

  Workaround: None.

- CSCtx94801

  show env fan command displayed as Ok even without power supply.

  Workaround: None.

- CSCty00734

  OSPF b/w CE-CE fails over Xcon if L3 Adj changes with no igmp snooping.

  OSPF failing over Xconnect between CE-CE connected via Xconnect. This occurs when there is a change in L3 Adjacency.

  Workaround: **clear xconnect** *peer vcid*

- CSCto61243

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

  Error messages with tracebacks appear on the console after flapping of interfaces happen. The error says cannot find di_index. This occurs when the interfaces are shut, forwarding stops on it. The destination indices (di_index) are set to illegal values owing to which these errors are seen.

  Workaround: None.

- CSCtq74742

  ACL with tcp established drops packets intermittently on ME3600X.

  ACL with permit tcp any any established applied on egress direction on middle switch drops packets randomly. This occurs on ME3600X.

  Workaround: Apply ACL with permit tcp any any established on ingress direction.

- CSCtx41690

  Outdiscards count huge value after **clear counter**.

  Workaround: None.

- CSCtx53479

  CPUHOG seen after reload "nrm_mpls_update_ingress_mpls_ttl_mode."

  Workaround: None.

- CSCtx89538

  Qos: out of resources when attaching input service-policy with marking.

  The following error message may appear on ME3800 running 15.1(2).EY1a when attaching ingress policy with marking to service instance:

  Qos: Out of internal resources

  %QOSMGR-3-LABEL_EXHAUST: Internal Error in resource allocation

  Workaround: None.

- CSCtx51914

  Static Multicast entry Expired after Reload.

  Workaround: None.

- CSCtx82882

  ESMC pkts are dropped when interface is configured with EVC.

  When evc is configured on interface of ME3600X, the ESMC pkts are not received but transmitted on that interface. This error occurs when SyncE with SSM is used on EVC.

  Workaround: Use **no switchport** or **dot1.q trunk** if possible.

- CSCtw75047

  ME-3600X-24CX: BIT-4-OUTOFRANGE messages seen on sending VPLS traffic from ME-3600X-24CX.

  Bit-4-OUTOFRANGE messages are seen on sending VPLS traffic from ME-3600X-24CX to ME3600. This occurs when VPLS traffic is sent between ME-3600X-24CX and ME3600.

  Workaround: None.

- CSCtx24601

  Port interface remains down on flapping etherchannel on EVC.

  Port channel interface goes down and never comes back up. Port channel configured on EVC and shut no shut the interface.

  Workaround: None.

- CSCtr61121

  Configuring backup link on already configured flink throws special chars.

  Junk characters displayed as ERROR message.

```
interface te0/1
switchport backup interface gig0/1
switchport backup interface gig0/2

%ERROR: TenGigabitEthernet0/1 is already a backup interface
%ERROR: 3n^]x^AI^S\n |n^^^D^CN^U^Kn^]/^CNxW
```

  While configuring backup link on already configured flink.

  Workaround: None.

- CSCtx68968

  Changing configuration under Service Instance causes forwarding to stop.

  Workaround: None.

- CSCty10180

  ME3600X: QoS Vlan grouping optimization for EVC scale per port.

  Number of qos tcams utilized is more if more service instances are configured on the port.

  QoS Tcams are exhausted if the service instance scale is configured per port.

  Workaround: None.

- CSCtx45945

  Tengig port flaps after about 15-30 hrs when 1000Base SFP is used.

  REP enabled TE port fails after some interval of time within 24 to 48 hours. This occurs when 1 Gig SFP is used in 10 Gig port.

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

- CSCtx68516

  SYS-2-BADSHARE tracebacks. This occurs on 500 IFMs on xconnect

  Workaround: None.

- CSCtx58755

  'Failed setting exception vector' message output.

  Upgrade ios from (12.2(52)EY3) to 15.1(2)EY1a, **Failed setting exception vector** message output.

  Workaround: None.

- CSCtx23929

  w2: Traceback seen @ Null swidb for if_number on SVI deletion.

  Workaround: None.

- CSCtx64473

  Cannot create routed PW on video template.

  Workaround: None.

- CSCty12140

  (S,G) not getting created on reconvergence.

  Workaround: None.

- CSCtr66941

  entPhysicalChildIndex variable is not returning properly in ME3800.

  Execute the below command from SNMP server:

  getmany <IP> entPhysicalChildIndex

  Workaround: None.

- CSCtx16060

  W1: OSPF is going down with too many retransmissions between RPW interface.

  OSPF remains in EXSTART state. This occurs when ospf is configured on a routed pseudowire.

  Workaround: None.

- CSCtw51052

  HSRPv2 pkts not forwarded over switch 10G Po, met programmed incorrectly.

  HSRP hello packets are dropped on the ME3600 when we have 2 ME3600 acting as switches between the HSRP boxes and have a Port channel connecting the 2 ME3600 with both the Tengig ports as its members. HSRP is configured on vlans.

  The issue is not seen consistently. It is seen only on a few vlans while the others may be working as expected.

  Workaround: Removing and re-adding the vlans fixes the issue.

  no vlan *vlan-id*> followed by **vlan** *vlan-id*

  Removing and adding the vlan from the port channel and its members also may fix the issue.

- CSCtx17484

  TE tunnel flaps if no route packet gets punted to CPU.

  TE tunnels flapping. This occurs when packets with no route for destination IP are pumped at high rate.

Workaround: Police the punted packets.

- CSCtx04483

  ME3800: Control Word not set when setting up Dynamic PW between ME3600/ME3800/7600.

  Control Word not set when setting up Dynamic PW between ME3600/ME3800 and 7600.

  Workaround: None.

- CSCtx09685

  ME3600/ME3800 crashes with latest xe36 nightly builds.

  Router crash. Events that trigger xconnect flaps/redundancy, mac flaps or in routing flap in some cases.

  Workaround: None.

- CSCty15571

  Crash observed on enabling adjmgr debugs using sdcli.

  Workaround: None.

- CSCtx97856

  Stale met entries remain after sending leaves.

  Workaround: None.

- CSCty18509

  Workaround: None.

- CSCtu32809

  ME3600/ME3800 IPv6 ACL: IPv6 Egress ACL issue with routed interface.

  With dual ip stack (ipv4 and ipv6), when ipv4 acl is configured on the interface in egress direction, ipv6 traffic is getting dropped. The error occurs when ipv4 and ipv6 ips are configured on the same interface. And the issue is seen for first ACL only, means for ACL label 1.

  Workaround: Assign some random acl on unsed interface, so that the acl consumes label 1. Then configure the actual acl on the dual stack interface.

- CSCtr84541

  BW distribution is getting affected upon class deletion in case of LLQ.

  Bandwidth distribution is getting affected upon dynamic changes in the policy-map.

  There are 2 scenario's which are affecting Bandwidth distribution upon class deletion w.r.t LLQ:

  Scenario1: Under child-policy, configure class cos1 with LLQ and the remaining 2 classes with BW. Then, remove class cos1 with LLQ and add back class cos1 with BW. This affects the BW distribution as the priority associated with class cos1 before removal is not getting cleaned.

  Scenario2: Under child-policy, configure class cos1 with LLQ and remaining 2 classes with BRP. Then, remove classes cos1 and cos2 and add back cos1 with BRP and cos2 with LLQ. Again BW distribution is affected with class cos3 not getting any BW share.

  Workaround: Remove the policy-map and apply it back on the interface.

- CSCts78737

  Box taking more time to boot-up when many ACEs configured.

  Taking more time to reload. Reloading when many ACEs are configured.

  Workaround: None.

- CSCtq29544

  ME3600/ME3800 QoS: Incorrect removal of efp service-policy on adding port-shaper.

  If a HQoS policy-map is applied on an EVC, parent bandwidth percent of 10%, child total bandwidth of 350 mbps. On adding the port_shaper with 500 Mbps at the port level the EVC policy-map gets removed. Ideally the port_shaper configuration should be rejected when there is an error in the configuration.

  In case of invalid config in port_shaper and EVC policy map, the last applied config should fail, instead the already attached policy-map is being detached.

  Workaround: Detach the policy-map, make valid configuration, and attach again.

- CSCtu32552

  Error message while changing port-shaper value on the fly.

  When increasing the port shaper value on the fly, the switch throws an error.

  EFPs are configured, and a port shaper policy is applied on the parent port. Under these conditions, when the shaping rate is increased the problem is seen.

  Workaround: Execute a **no shape** command, and then configure the desired rate.

- CSCtx02313

  Port mode EoMPLS config allowed with switchport configuration.

  Port mode EoMPLS config allowed with switchport config.

  Workaround: None.

- CSCtx46147

  W1: CFM not working in one direction over H-VPLS.

  Cfm ping fails when initiated on Mep on Efp bd when egress interface is a SVI or VFI PW and the remote mep mac is learned on the same.

  Cfm ping fails when initiated on Mep on Efp bd when egress interface is a SVI or VFI PW and the remote mep mac is learnt on the same.

  Workaround: None.

- CSCtx76780

  DHCP relay not working on ME3600 when using xconnect under VLAN int.

  DHCP relay does not work on ME3600. This problem is observed if we configure **ip helper-address** and an xconnect at the same time under the VLAN interface.

  Workaround: None.

- CSCty28796

  SNMP MIB for getting flash entries is not working in 15.1.

  show snmp mib | in flash on the router does not show any flash entries. Also snmpwalk for flash objects shows the following error:

  ```
  No Such Object available on this agent
  ```

  Workaround: None.

- CSCtx62137

  RSVP hellos sent but not received by neighboring device.

With cfm configured on access efp BD or switchport and SVI/VFI pw towards the core, RSVP pkts are not processed when the box has been running for sometime. The problem starts over time. This occurs with cfm configured on access efp BD or switchport and SVI/VFI pw towards the core, RSVP pkts are not processed when the box has been running for sometime. The problem starts over time.

Workaround: shut / no-shut the core interface should recover the RSVP. but not a practical solution as there would be outage on PW traffic.

- CSCtx91831

  SVI connected subnet not in the routing table.

  IP address of the SVI interface not installed in the routing table.

  When we have an IP address configured for the BD, the following sequence of configs puts the box in a state wherein the corresponding ip-address is not installed in the routing table.

```
no vlan <vlan-id>     --- same as the BD

Int vlan <vlan-id>
   shutdown           --- At this point the Int vlan goes down
   no shutdown

vlan <vlan-id>
```

  The issue seen only with SVI and BD efp. This is not seen for SVI and trunk ports.

  Workaround: A shut/no-shut of the interface vlan after adding the **vlan** *vlan-id* fixes the problem.

- CSCtx84823

  ME3800: CC Msg received on blocked port is catalogued.

  Workaround: None.

- CSCtx84823

  ME3800: CC Msg received on blocked port is catalogued.

  Workaround: None.

- CSCty32188

  On toggling igmp snooping traffic is stopped on switchport interfaces.

  Workaround: None.

- CSCtq36540

  Handle PIM notifications in ncef path for updating midchain adjacencies.

  Workaround: None.

- CSCtx45623

  ME3800: CFMoXConnect not working with control word set in mpls bindings.

- CSCty38599

  ME3600/ME3800 crash due to multicast.

  Node does not respond after network event or crash.

  Workaround: None.

- CSCtx76204

  Unicast flood fails on trunk portx for ME 3600.

Unicast is flooding between routed VLANs.

Workaround: None.

- CSCty28384

  ME3600/ME3800 QoS: Police command does not accept the confirm actions dynamically.

  Workaround: None.

- CSCtx61825

  Classification with **match vlan** fails for L3VPN IF more EVCs in BD.

  L3VPN/GRT egress traffic fails to get properly classified by **match vlan** command, when multiple attachment circuits / EVCs are present in the bridge domain, This occurs on unidirectional traffic, egress-only.

  Workaround: None.

- CSCty58403

  No S,G entries created after stopping traffic and sending leaves.

  This occurs on static-groups configured on loopback interface.

  Workaround: reactive workaround: flap the IIF OR **clear ip mroute ***

- CSCty40486

  SYS-2-INPUTQ seen on sending lbm and ltm on xconnect.

  SYS-2-INPUTQ tracebacks are seen on issuing lbm and ltm.

  Workaround: None.

- CSCty13314

  Traffic over data-MDT is not forwarded as its hitting on stale-TCAM entry.

  When there are TCAM entry churn (frequent add/delete), in qos, acl and ipv4te have tcam entry leaks shown, by tcam tracking error.

  ACL/QoS/IPv4 TE entry churn.

  Workaround: **clear ip mroute *** clears the issue for ipv4-te. None for QoS and Acl.

- CSCty54079

  OIF connected to RP is marked as A&F, hence traffic drop for 4 minutes.

  Multicast traffic will stop flowing with shut/no shut is performed on the interface or **clear ip mroute** command.

  Workaround: None.

- CSCty50421

  L2 protocols not tunneled over EVC xconnect.

  With control word set (C bit) explicitly in mpls bindings for the VC, l2pt tunnel over efp xconnect does not work.

  Workaround: Disable control word.

- CSCtx84501

  ME3800: Ethernet SLA Jitter probes do not work with EVC-BD configs.

  Workaround: None.

- CSCty14002

  L2protocol forward breaks tunneled L2 PDU.

  Adding l2protocol forward breaks tunneled l2protocol packets.

  Workaround: For the scenario mentioned in this ddts, removal of l2protocol forward on the EFPs will restore the end-to-end l2protocol neighbor.

- CSCty63544

  Packets are being s/w switched with scaled config.

  Multicast traffic getting sw switched with reload.

  Workaround: **clear ip mroute** may solve the problem.

- CSCty48220

  Having EFP and switchport under same vlan mcst traffic does not flow.

  Workaround: None.

- CSCty63252

  ME3600/ME3800 crashes in multicast.

  Node does not respond after network event or crash.

  Workaround: None.

- CSCtr04829

  DHCP/BOOTP: MLPPP Drops DHCP requests.

  A device configured with **ip helper-address** command drops packets because of a zero hardware address check. This symptom occurs when the hardware address is zero.

  Workaround: None.

- CSCty56256

  Tracebacks seen @ ncef_ios_adjacency_update_notification.

  Workaround: None.

- CSCty56197

  Enqueue back-pressure error reported.

  ME3800 completely stops forwarding traffic. Console is accessible during this period.

  There is no traffic egressing out any of the interface. Issue seen on both 12.2(22)EY1 and 15.1(2)EY1a. There is no high CPU or any general log messages. Switch appears completely isolated from a routing and spanning tree perceptive.

  Workaround: Switch reload is required.

- CSCtr28857

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

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

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

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

- CSCtr91106

  Command Authorization Fails for commands delivered over HTTP.

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

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

  This advisory is available at the following link:

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

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

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

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

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

- CSCtr49064

  Cisco IOS Software Reverse SSH Denial of Service Vulnerability.

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username.

  Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

Resolved Caveats for Cisco IOS Release 15.1 (2) EY2a

- CSCty59913

  A deny command on ACL does not work on ME3600.

  On ME3600, a deny command, included an implicit deny on ACL, does not work after an interfacedown/up which is configured for ip access-group xxx in. This issue is not applicable for SVI interface.

The interface which is configured for ip access-group xxx in is down/up with local shut/no shut, remote shut/no shut commands, or plug off/on the cable. This problem does not apply to ip access-group xxx out. It occurs regardless of an implicit or an explicit deny. Reconfiguring ACL; delete and configure ip access-group xxx in, and ip access-list, cannot recover the problem on 15.1(02)EY01a.

Workaround:

- For 12.2(52)EY04 Remove and reconfigure ip access-group xxx in.
- For 15.1(02)EY01a Reload the switch.

- CSCtz04090

  Ping to VRRP IP fails after VRRP Switchover.

  In a VRRP/HSRP setup, we could start seeing traffic from particular hosts getting dropped. Ping from the host to any device through the VRRP routers fails.

  This is usually seen after a VRRP/HSRP switchover. And the packet drops are because of some packet loop that is created between the routers running VRRP/HSRP.

  Workaround:

  A clear of the mac-table on the new VRRP MASTER usually restores the setup to working conditions. No other workaround known for this issue.

- CSCty93290

  Momentarily traffic loss of multicast traffic with qos config on EFP.

  Workaround: None.

- CSCty82717

  Packets are being software switched.

  Workaround: None.

- CSCty54319

  OSPF is not coming up between the CEs with pw and BD.

  OSPF and protocols using 224.0.0.x will not work btw CE-CE over a vlan.

  IGMP snooping disabled.

  Workaround: Toggle IGMP snooping twice.

Resolved Caveats for Cisco IOS Release 15.1 (2) EY3

- CSCty35724

  ME-3600X power-supply status is not correct.

  Cisco ME-3600X has one malfunctioning power-supply but ANA seems to show it with OK status.

  ANA query the following OID: 1.3.6.1.4.1.9.9.117.1.2.1.1.2 (cefcModuleOperStatus on CiscoEntityFRUControlMIB).

  ANA is not using ciscoEnvMonSupplyState (1.3.6.1.4.1.9.9.13.1.5.1.3) on ciscoEnvMonMIB, rather ANA uses cefcModuleOperStatus on CiscoEntityFRUControlMIB for many platforms, this issue need to be fixed in me3600x IOS for ANA to display the istatus as faulty.

  Workaround: Use the following instead:

  ciscoEnvMonSupplyState (1.3.6.1.4.1.9.9.13.1.5.1.3) on ciscoEnvMonMIB

- CSCtx47351

  Remote end reports alarm when ME3600x/3800x switch is configures as O/p src in T1 D4.

- CSCty80872

  ME 3600X - SNMP MIB "CISCO-ENTITY-SENSOR-MIB" does not work.

  snmp walk for the MIB 'CISCO-ENTITY-SENSOR-MIB', shows the error 'No Such Object available on this agent at this OID'. The ME 3600x switch is running 15.1(2)EY.

  Workaround: None.

- CSCtz35467.

  ME3600X QoS: P-map detached on line protocol down-->up transition

  QoS policy-map gets detached from interface on live protocol down-->up transition. This also occurs on reload, admin shut/no shut and interface flap.

  When QoS policy-map is applied at interface and more then 1 child has **priority + police cir percent x** configured.

  Workaround: To prevent this error use **police cir** *absolute* instead of **police cir percent x.**

  However if the error occurs use EEM applet/script.

  Note There is no error message in the syslog, only on console. At the time of writing it seems line protocol UP can be used as the trigger action for EEM.

- CSCty82363

  Tracebacks seen @ adjmgr_l3m_update_mcast_nh_with_cpu_q.

  Tracebacks with errors are seen on a ME3600x/3800x switch when it is interconnected with other switches. The errors are seen are seen when the interconnected switches are reloaded.

  Workaround: None.

- CSCts66156

  Need a way to disable DOM monitoring on ME3600.

  In order to avoid possible high under SFF8472 process with 3rd party SFP, DOM monitoring must be disabled.

  Workaround: None.

- CSCtz16622

  ME3600X drop Checksum 0xFFFF packet when act as a label disposition LSR.

  Cisco ME3600X acts as a label disposition Edge-LSR. When received MPLS packets with Checksum 0xFFFF that will keep continue drop with Ipv4HeaderErr and Ipv4ChecksumError at forwarding ASIC.

  This symptom is seen while label pop action at the Edge-LSR.

  Workaround: None.

- CSCtz14272

  SVI not installed in Multicast Routing Table as Incoming interface.

  Multicast forwarding stopped working after modifying SVI configurations.

Configure a new VLAN as EoMPLS VLAN (SVI+xconnect) or reload the device with EoMPLS VLAN. Change the SVI configuration from EoMPLS VLAN (SVI+xconnect) to normal L3 SVI with pim (SVI+IP+PIM). The SVI interface will not be installed in multicast routing table until you reload the device.

Workaround: Reload the device with SVI+IP+PIM configuration.

- CSCty42991

  Tracebacks observed on changing the spanning tree mode.

  The issue happens only with port-channel and is observed when the port-channel is added for the first time and spanning mode change following it.

  Workaround: None.

- CSCtz13451

  ME switch may crash running certain **show platform mpls handle** commands.

  ME 3800x and ME 3600X switch may experience CPUHOGs errors and then a Watchdog crash or memory corruption. The switch may crash when running many of the **show platform mpls handle** commands.

```
Switch# show platform mpls handle 262836664 ?
  BD_HANDLE              bd/el3idc_vlan handle
  L2VPN_L2_HANDLE        l2 tunnel intf handle
  L2VPN_PW_BIND_DATA     pw bind data
  LFIB_TABLE             LFIB TABLE handle
  PORT_HANDLE            port/met handle
  RW_HANDLE              Rewrite handle
  SW_OBJ_ADJACENCY       oce type SW_OBJ_ADJACENCY
  SW_OBJ_ATOM_DISP       oce type SW_OBJ_ATOM_DISP
  SW_OBJ_ATOM_IMP        oce type SW_OBJ_ATOM_IMP
  SW_OBJ_DEAGGREGATE     oce type SW_OBJ_DEAGGREGATE
  SW_OBJ_EGRESS_LABEL    oce type SW_OBJ_LABEL
  SW_OBJ_EOS_CHOICE      oce type SW_OBJ_EOS_CHOICE
  SW_OBJ_FIB_ENTRY       oce type SW_OBJ_FIB_ENTRY
  SW_OBJ_FRR             oce type SW_OBJ_FRR
  SW_OBJ_GLOBAL_INFO     oce type SW_OBJ_GLOBAL_INFO
  SW_OBJ_ILLEGAL         oce type SW_OBJ_ILLEGAL
  SW_OBJ_IPV4_FIB_TABLE  oce type SW_OBJ_IPV4_FIB_TABLE
  SW_OBJ_IPV6_FIB_TABLE  oce type SW_OBJ_IPV6_FIB_TABLE
  SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LABEL_ENTRY
  SW_OBJ_LABEL_TABLE     oce type SW_OBJ_LABEL_TABLE
  SW_OBJ_LOADBALANCE     oce type SW_OBJ_LOADBALANCE
  SW_OBJ_RECEIVE         oce type SW_OBJ_RECEIVE
```

  Workaround: None.

- CSCty87446

  w2: On changing split-horizon group secure mac address cleared from list.

- CSCtw55554

  Traceback at BIT-4-OUTOFRANGE: bit 0 is not in the expected range.

  Traceback at BIT-4-OUTOFRANGE: bit 0 is not in the expected range are thrown when running config is replaced by another file having around 1000 vlans. This is an intermittent traceback.

  Workaround: None.

- CSCtz27782

  Crash observed on defaulting EVC with OFM on BD configured on RLB slave.

Interface must in OAM RLB slave mode.

Workaround: None.

- CSCty91955

  Traffic not bridged between EVCs on same BD.

  L2-switched traffic loss within a BridgeDomain**,** routed traffic via an SVI experience no loss.

  BridgeDomain has both tagged and untagged EVCs. The issue should not happen with like-to-like scenario.

  Workaround: Make sure there is like-to-like (tagged-to-tagged or untagged-to-untagged) communication.

- CSCty72235

  NL3MD_STATs: MFIB_PLTF-3-ENTRY_HANDLE_BAD

  Reduction of dense mode mroutes from 4K to 100 trigger number of tracebacks on console.

  Workaround: Remove the 4K mroutes and then configure the 100 mroute fresh.

- CSCtn56206

  Unimplemented Function: local_port_mcast_supp_level

  Below error message is printed when a config change is made on an interface:

  ```
  Unimplemented Function: local_port_mcast_supp_level
  ```

  Interface command (config-if)#**storm-control multicast level** is configured on related interface.

  Workaround: Do not configure storm-control on related interface.

- CSCtz31610

  Only one **ip igmp snooping vlan** command loaded after switch reload.

  Customer found only one **ip igmp snooping vlan** command loaded after switch reload.

  1. Before IOS upgrade:

     ```
     ip multicast rpf backoff 10 1000
     ip igmp snooping vlan 303 static 224.0.1.101 interface Gi0/23
     ip igmp snooping vlan 303 static 224.0.1.103 interface Gi0/23
     ip igmp snooping vlan 303 static 224.0.1.102 interface Gi0/23
     ip igmp snooping vlan 303 static 224.0.1.104 interface Gi0/23
     no ip igmp snooping
     ```

  2. After IOS upgrade:

     ```
     no ip igmp snooping
     ip igmp snooping vlan 303 static 224.0.1.101 interface Gi0/23
     ```

  The Me3600 IOS upgrade from me360x-universalk9-tar.122-52.EY2a to me360x-universalk9-mz.151-2.EY2a.

  Workaround: Customer has to enter those commands again.

- CSCtz52736

  Unicast flood fails on trunk port x for ME 3600.

  Workaround: None.

- CSCty51088

  S,G is not getting created when the rcv interface starts sending traffic.

On a ME3600x/3800x box, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since not (S2,G) entry is formed. This error occurs as the receiver interface should already be a source interface for another multicast stream.

Workaround: None.

- CSCtz35467

  ME3600X QoS: P-map detached on line protocol down-->up transition.

  QoS policy-map gets detached from interface on line protocol down-->up transition happens on reload, admin shut/no shut and interface flap as well.

  This symptom is observed when QoS policy-map is applied at interface and more than one child has **priority + police cir percent x** configured.

  Workaround: To be preventive use **police cir** *absolute* instead of **police cir percent x**. To be reactive use EEM applet/script.

  Further Problem Description: There is no error message in the syslog, only on console. It seems that line protocol UP can be used as the trigger action for EEM.

- CSCty80872

  ME 3600X - SNMP MIB "CISCO-ENTITY-SENSOR-MIB" does not work snmp walk for the MIB 'CISCO-ENTITY-SENSOR-MIB', throws the error 'No Such Object available on this agent at this OID'. The ME 3600x running 15.1(2)EY.

  Workaround: None.

- CSCtx47351

  Remote end reports alarm when ME 3600x/ ME 3800x or ME 3600x-24cx are configured as O/p src in T1 D4.

- CSCty35724

  ME-3600X power-supply status is not correct.

  Cisco ME-3600X has one malfunctioning power-supply but ANA seems to show it with OK status. ANA query the following OID: 1.3.6.1.4.1.9.9.117.1.2.1.1.2 (cefcModuleOperStatus on CiscoEntityFRUControlMIB). ANA is not using ciscoEnvMonSupplyState (1.3.6.1.4.1.9.9.13.1.5.1.3) on ciscoEnvMonMIB, rather ANA uses cefcModuleOperStatus on CiscoEntityFRUControlMIB for many platforms, this issue need to be fixed in me3600x IOS for ANA to display the status as faulty

  Workaround: Use the following instead: ciscoEnvMonSupplyState (1.3.6.1.4.1.9.9.13.1.5.1.3) on ciscoEnvMonMIB.

- CSCty77582

  ME3800 QoS: Classification based on dscp does not work on EVC in SW Eompls.

  Traffic does not get classified in DSCP based class map for EVC in SW Eompls. When a policymap is applied to EVC in SW Eompls, DSCP based classification does not work.

  Workaround: None.

- CSCtj57866

  IGMP: traceback on int shut, when rep edge port is unconfigured.

  On a REP ring configuration., when no rep seg 100 edge no-neighbor primary command is issued, followed by a shut command., a traceback ensues with a BIT-4-OUTOFRANGE message. In a access-ring topology that has REP and multicast traffic, and when a no rep seg xxx edge no-neighbor

primary and shut commands are issued, a traceback is seen per vlan on which REP is configured with the following string: %BIT-4-OUTOFRANGE: bit 0 is not in the expected range of 1 to 1015. You may see this message one per vlan configured. Since port is shut and rep config removed, functionality is not affected.

Workaround:

- None.

or

- Issuing a shut on the rep edge port without unconfiguring the rep edge port config does not cause the traceback, and functionality is not affected.

- CSCty20330

  SNMP %SYS-2-MALLOCFAIL: Memory allocation of 2424504504 bytes failed SNMP requesting to large of a block of memory.

  ```
  Feb 15 23:44:28.285 CST: %SYS-2-MALLOCFAIL: Memory allocation of 2424504504 bytes
  failed from 0x15047BC, alignment 0 Pool: Processor Free: 803990516 Cause: Not enough
  free memory Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "SNMP
  ENGINE", ipl= 0, pid= 264
  ```

- CSCty47231

  ME 3600X/3800X QoS: Traffic starts dropping on removing the port-shaper.

  Traffic drops on removing the port-shaper. This issue is seen only when the policymap attach / detach is coupled with a link up / down, not seen on normal attach/detach. No issues with reload; policymap attached, and detached.

  Workaround: Default the egress interface, and reconfigure; traffic recovers.

- CSCtz12718

  MAC move from EVC BD to switchport does not work.

  Traffic drop when MAC is moved from EFP to switchport. This occurs with layer2 interface as EFP & switchport on two paths and layer3 interfaces as SVI and switching traffic from EFP to switchport.

  Workaround: None.

- CSCty99874

  ME3600 QoS: Ingress policing is done on the EVC which does not have QoS P.

  QoS: Ingress policing is done on the EVC which does not have QoS policy. When one EVC has a QoS policy, and another does not, the QoS policy show effect on the other also.

  Workaround: Attach a dummy policy to the other EVC; OR attach and detach a policy on the other EVC.

- CSCty18456

  ME3600-ARP request drop on ingress when sent to HSRP MAC address Not able to configure VRRP master IP as the interface IP. The Arp response packets destined for VRRP virtual mac is not processed by the master. When VRRP IP is configured as interface ip at the master side, The arp response will be destined for VRRP virtual mac. L2 packet destined for VRRP Mac is not processed by vrrp master, due to failure in arp resolution.

  Workaround: None.

- CSCtz08719

  Traffic stops on few BD on configuring split horizon.

With split horizon traffic does not flow on all BD. Traffic does not flow on all BD.

Workaround: None.

- CSCts45873

  CPU Hog messages for task SFF8472.

  Following error message is seen continuously and CPU spikes up:

```
*Aug 30 07:34:10.255: %SYS-3-CPUHOG: Task is running for (2004)msecs, more than
(2000)msecs (0/0),process = SFF8472.
-Traceback= 0x22C652Cz 0x22C23C8z 0x22C244Cz 0x275EC9Cz 0x275EF40z 0x275D91Cz
0x275DF10z 0x27BEE5Cz 0x27BF15Cz 0x27BFD04z 0x27C081Cz 0x27B53A0z 0x27B5D74z
0x1CC238Cz 0x1CC5328z 0x279FFCCz
*Aug 30 07:34:12.259: %SYS-3-CPUHOG: Task is running for (4008)msecs, more than
(2000)msecs (0/0),process = SFF8472.
-Traceback= 0x22C23C8z 0x22C244Cz 0x275EC08z 0x275EFB0z 0x275E25Cz 0x27BEEA4z
0x27BF15Cz 0x27BFD04z 0x27C081Cz 0x27B53A0z 0x27B5D74z 0x1CC238Cz 0x1CC5328z
0x279FFCCz 0x27A010Cz 0x1C4CFA8z
```

  This occurs when inserting SFP in a port.

  Workaround: Insert the sfp and then reload the box.

- CSCtw79171

  adjmgr_l2_create Platform Asserts with VPLS/L2VPN configs.

  Platform Asserts at adjmgr_l2_create. There is excessive flapping of a link.

  Workaround: None.

- CSCua44510

  Capability addition for mpls te node protection.

- CSCtx54990

  Static MAC address removed from config on reload ME-3600x.

- CSCtz67403

  ME-3600 as Core SWITCH Dropping all BPDU coming in QnQ Tunnel.

  This occurs where the ME-3600 is Core, and ME-3400 are Edge Switches.

  Workaround: None.

- CSCtz45487

  Packet loss seen when modifying allowed vlans on trunk.

  REP flaps when modifying allowed vlans on REP enabled trunk.

  This occurs under the following conditions

  - Vlan dot1q tag native must be configured globally.
  - Issue does not occur when native vlan is 1 on REP trunk.
  - Issue is seen on 15.2(2)S, 15.1(2)EY2a and earlier 15.1(2) releases.
  - Issue is not seen on 12.2(52)EY4 and earlier 12.2(52)EY releases.

  Workaround:

  - Remove vlan dot1q tag native global config.
  - Change to native vlan 1 on the REP enabled trunks.
  - Change to 12.2(52)EY train.

- CSCtz28304

  ME 3600X/ME 3800X REP Flaps with bfd configured on the node.

  Workaround: None.

Resolved Caveats for Cisco IOS Release 15.1(2)EY4

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

Note The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtj58507

  OSPFv3 "router-id" configuration is lost after SSO.

  IPv6 OSPF "router-id" configuration is lost after switchover.

  Conditions: The router-id command does not get sync to standby RP if the operational router ID on the primary RP is the same as what is coming from the router-id command. Specific to OSPFv3.

  Workaround: If operational router ID is not the same as the "router-id" then the command is synced to the standby RP.

- CSCtj47822

  State issues and memory leaks with standby RP.

  The standby RP is stuck in standby_issu_negotiation_late state after a switchover and does not come to SSO. Also, memory leaks are observed at tid_cmn_add_or_find_port_info.

  Conditions: The symptom is observed during the peer (standby RP) reset or switch-over.

  Workaround: None.

- CSCtj55680

  On the Route Server, when an update-group member moves out of the update-group and joins it back again, unnecessary withdraws or duplicate updates occur.

The Route Server withdraws the prefixes advertised to its route-server client when the route-server client goes out and then gets back into the same format group.

Conditions: In a rare case when the peer goes out of the update-group and then gets back into the same update-group on the Route Server, then the Route Server withdraws the prefixes advertised by it to its clients.

Workaround: Running the following command pushes the withdrawn prefixes back to the route-server client:

```
clear ip bgp <route-server-client address> soft out
```

- CSCtn58128

  BGP process crashes with watchdog timeout on route flap.

  The BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: Issue may be triggered by route-flaps in a scaled scenario where the route reflector may have 4000 route reflector clients and is processing one million+ routes.

  Workaround: Ensure that no logging console is configured.

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCtq07761

  Session flap due to malformed update for IPv6 Unicast updates.

  Updates incorrectly contain a label for IPv6 unicast AFI/SAFI encoding, causing a session flap at the peer. BGP RR is configured with a send label to the route-reflector-client, but the outbound route-map does not have a set MPLS label. Each time the withdraw is sent, it is encoding with the MPLS label in the MP_UNREACH_NLRI while the SAFI is set to 1 (unicast without label). This is categorized as an illegal network, (or a malformed update).

  Conditions: The symptom is observed when the following conditions are met:

  - neighbor x route-reflector-client
  - neighbor x send-label
  - neighbor x route-map Map out
  - route-map Map there is no set MPLS label

  Workaround: Add the set MPLS label in the outbound route-map.

- CSCtq18459

  CLI errors for the command bgp confederation peer <as-number>.

  If you enter the bgp confed peer <cr> command, it is accepted. On an HA system, if you then type the following command: no bgp confed peer <cr>, you may cause standby to reload. If you enter the following command: bgp confed peer 1 2 3 xyzfsasdf any-text, you'll get an unrecognized command error, but the effect is shown in "show run": "bgp confed peer 1 2 3".

Conditions: Typing in command syntax that is technically allowed, but semantically wrong.

Workaround: None.

- CSCtq48455

  VLAN goes down on 10G interface after flex link switchover

  After a Flex Link failover, all VLAN SVIs associated with VLANs forwarding on the Flex Link interfaces go down.

  Conditions: The symptom is observed with Flex Links configured with VLAN SVIs.

  Workaround: Remove the Flex Links and then reconfigure them.

- CSCtq62759

  ISIS LSP not regenerated when interface shuts down.

  The CLNS routing table is not updated when the LAN interface with CLNS router ISIS configured shuts down because ISIS LSP is not regenerated. The CLNS route will be cleared after 10 minutes when ISIS ages out the stale routes.

  Conditions: The symptom is observed only when the CLNS router ISIS is enabled on a LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Run one of the following commands:

  ```
  clear clns route
  clear isis *
  ```

- CSCtq91442

  PBR Multiple Tracking objects missing FM notification.

  When configured for the PBR Multiple Tracking feature, the traffic is punted to software.

  Conditions: The symptom is observed with Cisco 7600 routers with IOS releases supporting the PBR Multiple Tracking feature.

  Workaround: Add a dummy route-map sequence to trigger a notification. Care should be taken that this dummy route-map will handle traffic which are not matched in other route-map sequences.

- CSCtq92182

  eBGP neighbor stays in Idle thru IPv4-Compatible IPv6 Tunnel intf.

  An eBGP session is not established.

  Conditions: The symptom is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq96329

  BGP withdraws are not sent when bgp deterministic-med is configured.

  Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: The symptom is observed only when bgp deterministic-med is configured.

Workaround: Disable deterministic med in the network/AS by issuing the no bgp deterministic-med command and then the clear ip bgp * command or perform a hard reset of the BGP session to remove any stale prefixes. It is also recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

- CSCtz00430

  Static route removed on removing replacing connection on management INTF.

  The static route is removed from the routing table.

  Conditions: The symptom is observed when pulling out and replacing a connection to the management interface.

  Workaround: There are two possible workarounds:

  - Default the management interface and reconfigure IP.
  - Do a shut and no shut on the management interface through the CLI.

- CSCtz35061

  Flexlink switchover causes VLAN to not be allowed in trunk link.

  Conditions: This issue is related to flexlink switchover caused by instantaneous link flapping.

  Workaround: None.

- CSCtz48867

  multicast traffic cannot be forwarded via an etherchannel between 2 Cisco ME 3600X

  In the customer network, this problem was triggered under the following situation:

  ```
  Active WG          Standby WG
       |                    |
  Active BR -------- Standby BR
       |
    Client
  ```

  Active BR and Standby BR are two Cisco ME 3600X switches. The link between the two Cisco ME 3600X switches is an etherchannel (two member ports). Multicast traffic from the Active WG and Standby WG flow down the path. The multicast clients join the multicast group via an SVI interface in the two switches and the L2 etherchannel between the switches trunks that particular VLAN.

  In a normal situation, the client should be able to receive multicast streams 224.0.1.x (from Active WG) and 224.0.127.x (from Standby WG). After the Active BR is reloaded, multicast streams 224.0.127.x can no longer be forwarded from the Standby BR to the Active BR.

  Conditions: This symptom occurs when the Active BR is reloaded.

  Workaround: Run the command clear ip mroute * on the standby BR.

- CSCua16046

  H-VPLS packet loss issue.

  Some packets are dropped when multiple streams are merging on the Cisco ME 3600X and Cisco ME 3800X switches. Sometimes, packet drops are observed with a single stream as well.

  Conditions: The symptom is observed with smaller size packets, such as 64-512 bytes.

  Workaround: The workaround depends on the release. In some releases, running the command no ip gmp snooping solves the issue.

- CSCua36075

  On the Cisco ME 3600X, BFD does not come up on the SVI for the first time on the box.

  Conditions: On a fresh router boot, configure bfd all-interface on the ospf process, then platform bfd allow-svi and bfd interval 50 min_rx 50 multiplier 3 on the SVI. BFD neighbors are not shown in sh bfd neighbors. On deleting the OSPF or removing the bfd configuration from the OSPF, bfd comes up fine.

  Workaround: None.

- CSCua83876

  Multicast streams stop being forwarded with message MET FULL ERR.

  Some multicast streams may be stopped being forwarded or new multicast streams cannot be joined. Also, the following message appears:

  ```
  allocate_l3m_port_fcje: RPF PASS nh_hdl(0xD2668C0) MET FULL ERR
  ```

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

  Workaround: None. However, a reboot is required to clear the situation temporarily.

- CSCua48584

  ME3600X ARP entry becomes incomplete after clear specific entry.

  The Cisco ME 3600X's ARP resolution may fail after flexlink switchover.

  Conditions: The symptom is observed on the Cisco ME 3600X running Cisco IOS Release 15.2(S) or Cisco IOS Release 15.2(2)S1 with flexlink configured.

  Workaround: Shut the active port of the flexlink pair. In other words, do a manual switchover through CLI.

- CSCua84606

  l2pt CPU forwarding with more than 2 VLANs fails.

  With L2PT tunnel or forwarding, the Cisco ME 3600X switch or the Cisco ME 3800X switch cannot process more than two VLAN tags. Such packets get dropped.

  Conditions: The symptom is observed with L2PT tunnel or forwarding.

  Workaround: None.

- CSCua96392

  HSRP stops working after shut/no shut on a port channel member.

  Conditions: The symptom is observed when a port-channel (with at least 2 members) member is shut.

  Workaround: None.

- CSCua98421

  CFM does not work when QoS entries are already programmed.

  RMEPs from an ASR9K are not learned on a Cisco ME 3800X with CFM running over a xconnect. The ASR9K does learn the RMEPs from the 3800.

  Conditions: QoS is enabled on the Cisco ME 3800X prior to enabling CFM.

  Workaround: Apply the CFM configuration before QoS or reload the switch with both QoS and CFM enabled in the configuration.

- CSCub23055

Cisco ME 3800X crashes while trying to remove service instance.

When a Cisco ME 3800X is running 15.1(2)EY3 software, the system will reload.

Conditions: System reloads only when removing the EVC service instance that is configured with the bridge-domain split-horizon group option.

Workaround: Before removing the EVC service instance, remove the split-horizon group option from the bridge-domain command first.

Related Documentation

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

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

ME 3600X switch:

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

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

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

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

These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

---

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