

Bugs for Cisco IOS Release 15.3(1)S

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the [Cisco Bug Search Tool](#). This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug.

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results

**Note**

If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

This section consists of the following subsections:

- [Resolved Bugs—Cisco IOS Release 15.3\(1\)S2, page 179](#)
- [Resolved Bugs—Cisco IOS Release 15.3\(1\)S1, page 199](#)
- [Open Bugs—Cisco IOS Release 15.3\(1\)S, page 218](#)
- [Resolved Bugs—Cisco IOS Release 15.3\(1\)S, page 235](#)

Resolved Bugs—Cisco IOS Release 15.3(1)S2

- CSCej00344

Symptoms: A router may reload unexpectedly when opening a terminal session.

Conditions: This can be seen on any platform. It can be seen when starting any terminal session from the router, including a mistyped command which the router by default will try to resolve as an address to telnet to.

This bug is not specific to X.25 config and is seen when initiating an outbound telnet/ssh/rlogin session from the device. Occurs when there are multiple outbound sessions from the same terminal (console, vty).

Workaround: There is no workaround.

- CSCsm40779

Symptoms: A router may go into initial configuration dialog on bootup.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(11)T2 with the c7200p-adventerprisek9-mz image.

Workaround: There is no workaround.

- CSCth03648

Symptoms: Cisco 2960 and 3750 series switches running Cisco IOS Release 12.2 (53)SE1 may crash.

Conditions: This symptom is observed if two traps are generated by two separate processes, and if one process suspends and the other process updates some variables used by the first process.

Workaround: Disable all snmp traps.
- CSCtq26296

Symptoms: Router crashes with DLFI configurations.

Conditions: The symptom is observed while doing a shut/no shut.

Workaround: There is no workaround.
- CSCts60458

Symptoms: There is a memory leak in PFR MIB.

Conditions: This symptom occurs when PFR is configured.

Workaround: There is no workaround.
- CSCtx50235

Symptoms: During a crash on the Cisco Catalyst 6500, the normal crash information from the crashinfo files may be missing due to the crashes showing the Routing processor (RP) being reset by the Switching Processor (SP) and the RP crashinfo also showing the RP being reset by the SP. This bug addresses this serviceability issue and it has nothing to do with the root cause of the crash itself.

In a majority of cases, the crash has been a single-event crash and has not repeated.

Conditions: Conditions of this symptom are not known currently. At this point, it is believed that the real fault of the crash belongs to the SP.

Workaround: There is no workaround.
- CSCty07538

Symptoms: TCP sessions get reset intermittently when NAT is configured with more than 1500 translations.

Conditions: This symptom occurs in the Cisco Catalyst 6500-Sup720/Sup32 when NAT is configured with more than 1500 translations.

Workaround 1: Remove NAT.

Workaround 2: Force packets coming to RP on the NAT interfaces to be process switched by configuring “no ip route-cache” on the NAT interfaces.
- CSCty59423

Symptoms: Memory leak seen with following messages:

```
Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "VOIP_RTCP", ipl= 0,
pid= 299 -Traceback= 0x25B1F0Cz 0x25AB6CBz 0x25B1029z 0x46C02Ez 0x46C89Bz 0x46BCC2z
0x471D12z 0x43EF59Ez 0x43DD559z 0x43DCF90z %SYS-2-MALLOCFAIL: Memory allocation of 780
bytes failed from 0x46C02E, alignment 32
```

Conditions: The conditions are unknown.

Workaround: There is no workaround.

- CSCtz53214

Symptoms: The “clear counter pseudowire <#>” commands do not clear the pseudowire specific counters.

Conditions: This symptom is reported to be present in all Cisco IOS Release 15.X(S) versions.

Workaround: Issuing global clear count (“clear counters”) will clear counters including pseudowire specific counters.
- CSCua26981

Symptoms: A Cisco ASR router may crash due to a CPU Watchdog upon invocation of “show ip eigrp neighbor detail”.

```
sh ip eigrp nei detail
<snip>
ASR1000-WATCHDOG: Process = Exec
%SCHED-0-WATCHDOG: Scheduler running for a long time, more than the maximum
configured (120) secs.
-Traceback= ...
===== Start of Crashinfo Collection =====
```

Conditions: This symptom occurs when the Cisco ASR router is experiencing rapid changes in EIGRP neighborship, such as during a flap. One way to artificially create this scenario is to mismatch the interface MTU.

Workaround: There is no workaround.
- CSCua76157

Symptoms: BGP routes are displayed.

Conditions: This symptom occurs after removing the “send-label” from PE.

Workaround: There is no workaround.
- CSCua78782

Symptoms: Authentication of EzVPN fails.

Conditions: The symptom is observed with BR-->ISP-->HQ.

Workaround: There is no workaround.
- CSCub19185

Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

Workaround: There is no workaround.
- CSCub40547

Symptoms: ES+ module is crashing with “%NP_DEV-DFC1-2-WATCHDOG: Watchdog detected on NP 0” error.

Conditions: The issue is specific to the type of packet and its content which is unique when vidmon is configured.

Workaround: Remove vidmon configuration.
- CSCub45763

Symptoms: The device crashes due to SYS-2-FREEFREE and SYS-6-MTRACE messages while a CDP frame is being processed.

Conditions: This symptom occurs when CDP is in use.

Workaround: Disable CDP using the **no cdp run** command.

Note: If the device in question relies on or supports a phone or voice network, this is not a valid workaround.

- CSCub60422

Symptoms: The ME-3600X-24CX-M box crashes on executing the **diagnostic start test all** command.

Conditions: This symptom occurs on executing the **diagnostic start test all** command.

Workaround: There is no workaround.

- CSCub72198

Symptoms: Executed CLI fails to sync to standby and results in standby reload.

Conditions: This occurs when the following conditions are met:

1. Active and standby are running different version of IOS image.
2. The CLI being applied is not PRC compliant, meaning that this CLI does not return a valid parser return code.

Workaround: Avoid applying CLIs that are not PRC compliant during image upgrade or downgrade.

- CSCub93937

Symptoms: PfR “OER border router” process might report exception and the router reloads under stress traffic.

Conditions: The symptom is observed with a PfR configuration with scaling traffic-class actively, and stress control traffic between PfR MC and BRs.

Workaround: There is no workaround.

- CSCub95365

Symptoms: An ES+ crashes upon the dynamic addition/deletion of class-maps.

Conditions: The symptom is observed with the dynamic addition/deletion of class-maps of a policy applied in scale number of PC EVCs.

Workaround: There is no workaround.

- CSCuc05929

Symptoms: After a reload, sometimes the MPLS forwarding function on some interfaces is not enabled. Some interfaces that were configured with “mpls ip” and link-state-up do not show with the “show mpls interface” command. This issue depends on a timing of the interface up.

Conditions: Sometimes the issue occurs after a router reload or SIP/SPA reload. It is not affected when you configure “mpls ip” on an interface, admin-shutdown/no shutdown, and link-flap.

Workaround: There is no workaround. When the issue occurs, do an admin-shutdown/no shutdown on the affected interface or disable/re-enable MPLS on the interface.

- CSCuc09483

Symptoms: Under certain conditions, running a TCL script on the box, may cause software traceback and reload of the affected device.

Conditions: Privilege 15 user may run TCL commands that may lead to an affected device reloading.

Workaround: There is no workaround.

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 3.8/3.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C> No CVE ID has been assigned to 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

- CSCuc12685
Symptoms: Address Error exception is observed with ccTDUtilValidateDataInstance.
Conditions: This symptom is observed with ccTDUtilValidateDataInstance.
Workaround: There is no workaround.
- CSCuc23542
Symptoms: The PXE client network boot fails when an ME3600 running 152-4.S is the DHCP relay agent.
Conditions: This symptom occurs when the ME3600 changes the option 54 "DHCP Server Identifier" address to its own IP address in the DHCP offer received from the PXE DHCP server. This causes the client to send the PXE boot request (port 4011) to the ME3600 instead of the PXE server.
Workaround: Downgrade ME3600 to Cisco IOS Release 15.1(2)EY.
- CSCuc32721
Symptoms: Traffic is failing to map-cache entries that have IPv6 locators.
Conditions: The symptom is observed when, although IPv6 is disabled, in map-cache entries with IPv6 RLOCs, those RLOCs are shown as "up".
Workaround: Enable IPv6 unicast-routing; then RLOCs are marked no-route.
- CSCuc42518
Symptoms: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that could allow a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition, while trying to process certain RTCP packets during media negotiation using SIP.
Conditions: Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.
Workaround: Increase the interface input queue size. Disable Video if not necessary.
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 4/3.1:
<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C> CVE ID CVE-2012-5427 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
- CSCuc44306
Symptoms: The IPv6 HbH packets get punted to RP as a result of HbH rate-limiter not working.
Conditions: This symptom is observed when IPv6 HbH packets hit the bridged interface on SIP400/SIP200 with IPv6 HbH rate-limiter configured.
Workaround: There is no workaround.

- CSCuc46087
Symptoms: CUBE does not send a response to an early dialog UPDATE in a glare scenario.
Conditions: This symptom occurs when CUBE receives an early dialog UPDATE when it sends 200OK to INVITE and expects ACK.
Workaround: There is no workaround.
- CSCuc47879
Symptoms: Removing the channel group configuration on a CEM controller causes the device to hang in a particular scenario.
Conditions: This symptom is observed when the following steps are performed:
 1. Configure CEM group (CESoPSN or SAToP) on a controller.
 2. Configure channel group on this controller with same time slots used in step 1 for CEM group.
 3. Remove channel group configured in step 2.
 Workaround: Perform hard reboot of the device.
- CSCuc54300
Symptoms: During an SSO or an initial bootup, standby fails and reboots again.
Conditions: This symptom occurs when a reload or SSO is performed.
Workaround: There is no workaround.
- CSCuc59858
Symptoms: Valid dynamic authorization requests which are not retransmissions are marked as retransmission.
Conditions: This may occur when valid dynamic authorization requests with the same RADIUS packet identifier is sent from different source ports.
Workaround: There is no workaround.
- CSCuc60297
Symptoms: Redistribute or source (network statement) VRF route into BGP. BGP VRF prefix with next hop from global, the next-hop will be inaccessible.
Conditions: This symptom is observed when redistribute VRF routes into BGP with global NH.
Workaround: There is no workaround.
- CSCuc61302
Symptoms: The symptoms for XE38, XE37 and mcp_dev are different for this DDTS. On mcp_dev, VPLS PW is not coming up, but on XE37 and XE38, static mac commands are missing after a reload.
Conditions: This occurs only on reload. The configured static mac commands are missing after a reload.
Workaround: There is no workaround other than re-entering the static mac commands.
- CSCuc69342
Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback:
-Traceback= 5B01805 46158ED 45F4F57 45BB19E 45BA1CF 451D6DC 4525549 45252D9 4519C30 45196A9 4778FFD
After the reload from the crash, it may take some time before it crashes again.
Conditions: This symptom occurs when CUBE receives the SIP REFER message with the Refer-To header having no user part.

- Workaround: There is no workaround.
- CSCuc73473

Symptoms: The IPv6 default route is not redistributed in BGP(VRF).

Conditions: This symptom occurs when the OSPFv3 “default-information originate always” is configured in the same VRF.

Workaround: To clear the issue, enter “cle ip bg *”. To avoid the issue, remove “default-information originate always” from OSPFv3 in the respective VRF.
 - CSCuc76309

Symptoms: Crash on RP2: be_ip_arp_retry_.

Conditions: The symptom is observed when the physical interface is shut until all IPsec SAs are deleted, then a no shut is done.

Workaround: Disable ARP retry feature. To disable ARP retry feature, the following two commands are needed:

no ip arp incomplete enable; and

no ip arp incomplete retry.
 - CSCuc78328

Symptoms: SP crashes followed by an RP reset.

Conditions: This symptom occurs when multicast-enabled (PIM) tunnels are protected with IPsec.

Workaround: There is no workaround.
 - CSCuc87208

Symptoms: The router crashes while configuring inherit peer-session.

Conditions: A peer-session template is inheriting from another peer-session template where the inherited template has the “ha-mode sso” configured. For example:

```
router bgp 1
  template peer-session ps.rmtAS.10000
  remote-as 10000
  exit-peer-session
  template peer-session ps.rmtAS.10000.sso
  inherit peer-session ps.rmtAS.10000
  ha-mode sso
  exit-peer-session
  template peer-session ps.rmtAS.10000.sso.bfd
  inherit peer-session ps.rmtAS.10000.sso
```

Workaround: There is no workaround.
 - CSCuc96631

Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

Workaround: Use Cisco IOS Release 15.2(2)T.
 - CSCuc97995

Symptoms: The PPPoE subscribers stop coming online.

Conditions: This symptom is not observed under any specific conditions.

Workaround: The following workaround are used to resolve the issue:

1. Remove radius attribute “ip mtu x” from the user profile.
 2. Remove accounting list from the service applied to the subscriber.
- CSCud03250

Symptoms: Large TCP data transfers take longer than expected (about a 40% increase in time). In particular, initial BGP convergence for a full internet routing table after reload is known to increase by several minutes. Performance degradation was seen starting the XE37 throttle build 09/18 (BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025).

A comparison of sniffer traces of affected and unaffected traffic will show that in impacted versions of Cisco IOS, TCP more frequently probes the path MTU, and that when the larger packets are dropped, it treats these drops as indicating the presence of network congestion, and slows down the rate of data transmission.

Conditions: This symptom is observed when the user tries with the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label and the performance number is still good, but the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025 label image shows much higher performance numbers in the order of 400 seconds. This issue is seen when the user also tries with the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label.

Workaround: The underlying problem is caused by changes in the TCP path MTU discovery algorithm. Disable TCP path MTU discovery for affected BGP neighbors. Depending on the release, this is done by configuring the following:

neighbor x.x.x.x transport path-mtu-discovery disable or
no neighbor x.x.x.x transport path-mtu-discovery

Note that the use of this workaround may have other negative performance consequences caused by packet fragmentation, and there may be a need to tune interface MSS.

- CSCud04998

Symptoms: The Cisco 7600 LC crashes when the frame interval is set less than 25 ms and aggregate interval is greater than 10.

Conditions: This symptom is observed when the frame interval is set less than 25 ms and aggregate interval is greater than 10.

Workaround: Do not set the frame interval to less than 25ms.

- CSCud08595

Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to multiframe established.

Conditions: This symptom occurs when “voice-class busyout” is configured and the controller TEI comes up before the monitored interface.

Workaround: Remove the “voice-class busyout” configuration from the voice-port.

- CSCud11078

Symptoms: Removal of the service instance on the target device causes a crash.

Conditions: Not consistently reproducible on all configurations as the underlying cause is a race condition.

Workaround: De-schedule the probe before removing the service instance.

- CSCud11627
Symptoms: SUP720 supervisor module may hang in ROMMON after the module reset triggered by TM_DATA_PARITY_ERROR.
Conditions: The issue is observed after a module reset triggered by TM_DATA_PARITY_ERROR.
Workaround: Power off/power on the router.
- CSCud19593
Symptoms: DHCP-Restart-session does not get synched to the standby for dual-stack session.
Conditions: First, a dual-stack session is created on the router (one stack should be DHCPv4) and then cleared. Then the DHCP-session is restarted.
Workaround: There is no workaround.
- CSCud22038
Symptoms: When a PC is moved between two VLAN ports (on one port, ISG is enabled and the other port is non-ISG) several times by its LAN cable connection on the L2SW that is connected to the Cisco ASR 1000 router, the PC is unable to receive DHCP OFFER due to the wrong VLAN ID from the DHCP server on the Cisco ASR 1000 router.
Conditions: This symptom is observed with Cisco IOS Release 15.2(4)S1.
Workaround: There is no workaround.
- CSCud22222
Symptoms: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.
Conditions: Issue may happen if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.
Workaround: Configure metric-style wide for both levels (by default).
- CSCud28541
Symptoms: SP crashes on doing **no mpls ip** followed by **shut** on port-channel acting as core link for scaled VPLS and EoMPLS setup.
Conditions: In case of VPLS going over port-channel protected by IP-FRR, when the port-channel is shut the AToM VC is going down and getting created again. Also the PPO object is getting created afresh. The VC going down is not handled for VPLS case and AToM VC’s pointer are still stored in IP-FRR’s EoMPLS list which is getting access and hence crashing.
Workaround: There is no workaround.
- CSCud33159
Symptoms: Excessive loss of MPLS VPN traffic and high CPU utilization is observed due to the process switching of MPLS traffic over the ATM interface.
Conditions: This symptom occurs when MPLS is enabled on the ATM interface with aal5snap encapsulation.
Workaround: There is no workaround.
- CSCud35336
Symptoms: There is a trace back without any traffic loss.
Conditions: This symptom occurs when you disable and enable multicast routing on vrf without any delay.

Workaround: If disable/enable of multicast routing is given with a time gap, this issue does not occur.

- CSCud35462

Symptoms: Multicast traffic does not flow over MVPN.

Conditions: The symptom is observed when SVI is used as the core interface.

Workaround: Use a physical interface as the core interface.

- CSCud38774

Symptoms: Router is showing CPU utilization at 99%. LDAP seems to be hogging the CPU process.

Conditions: This issue can occur randomly at any point of time where NTLM authentication is deployed. This issue is observed only when the server is not able to handle the churn of requests and requests are being stuck at Bind On-Going state, which can be verified with **show ldap server *server-name* connections**.

Workaround: Clearing LDAP server connections helps in resolving this issue:

clear ldap server *server-name*.

- CSCud41058

Symptoms: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.

Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in **distribute-list route-map *name* out**.

Workaround: Clear the EIGRP process or re-advertise the route.

- CSCud45100

Symptoms: Router goes down due to a crash.

Conditions: The symptom is observed when you have CFM over xconnect with PC in the core and run Y1731 DMM on it.

Workaround: There is no workaround.

- CSCud50768

Symptoms: For an elected BSR in an HA system, shortly after the standby becomes active, there is a 2-3 minutes period with no BSR messages sent.

Conditions: This symptom occurs when there is an HA switch on the elected BSR.

Workaround: There is no easy workaround other than not configuring a C-BSR on an HA system.

- CSCud62774

Symptoms: The values reported for “application media packets rate variation [sum]” may be incorrect. The functionality of Media Rate Variation TCA (Threshold Crossing Alarm) may also be impacted by this.

Conditions: This symptom is observed when the user wants to obtain MRV metrics by including the following command in the Performance Monitor flow record configuration:

application media packets rate variation [sum]

Workaround: There is no workaround.

- CSCud65119

Symptoms: A crash may occur while using GETVPN with fragmented IPv6 traffic.

Conditions: This symptom occurs when IPv6 IPsec is used. This issue is triggered by fragmented IPv6 packets.

Workaround: There is no workaround.

- CSCud66669

Symptoms: On the Cisco 7200, the tunnel is established correctly and encryption and decryption occur correctly. However, after decryption, the packet is not punted to the iVRF in which the tunnel interface resides, leading to a broken IPsec-DataPath.

Conditions: This symptom is observed with the Cisco 7200 with VSA under the following conditions:

- Tunnel (GRE/mGRE) in an iVRF with Tunnel protection configuration.
- iVRF not equal to fVRF.

Workaround: This issue has been observed with Cisco IOS Release 15.0(1)M9 and Cisco IOS Release 12.4(24)T8, so downgrade might be an option. There is no known configuration-related workaround yet, although software crypto will work just fine.

- CSCud71606

Symptoms: The LSMPI Tracebacks errors are seen while clearing IP routes multiple times.

Conditions: This symptom is observed under the following conditions:

- Configuring OSPF.
- Has more than 1000 OSPF neighbors, which will make OSPF LSU packet get fragmented.
- Clear ip ospf process * and OSPF will send LSU packet, which triggers this error message.

Workaround: There is no workaround.

- CSCud71773

Symptoms: The **cost-minimization** test command is not accepted.

Conditions: This symptom is observed with the **cost-minimization** test command.

Workaround: There is no workaround.

- CSCud79067

Symptoms: The BGP MIB reply to a getmany query is not lexicographically sorted.

Conditions: This symptom is observed when IPv4 and IPv6 neighbor IP addresses are lexicographically intermingled, for example, 1.1.1.1, 0202::02, 3.3.3.3.

Workaround: There is no workaround.

- CSCud84695

Symptoms: Serial interface with FRF.12 feature is not coming up.

Conditions: This symptom is observed when the flags related to FRF.12 feature are not properly updated in Elocal UCODE table.

Workaround: There is no work around.

- CSCud86954

Symptoms: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache

entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn’t get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

The following is sample output when all cache entries are lost:

```
Router#sh flow monitor FNF-MON stat
Cache type:                               Normal
Cache size:                               4096
Current entries:                           0
High Watermark:                            882

Flows added:                               15969
Flows not added:                           32668
Flows aged:                                15969
- Active timeout      ( 1800 secs)         0
- Inactive timeout    (   15 secs)        15969
- Event aged          0
- Watermark aged      0
- Emergency aged      0
```

Conditions: This symptom occurs when all of the following are true:

- Flexible Netflow is enabled on a DMVPN tunnel interface.
- Local policy-based routing is also enabled on the router.
- Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

Workaround: Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.

- CSCud90950

Symptoms: Multicast traffic might not flow through when the P2P tunnel is the incoming interface in the Cisco 7600 router.

Conditions: This symptom occurs in the Cisco IOS Release 12.2SREx and Cisco IOS Release 15.0x.

Workaround: Shut and no shut of the P2P tunnel interface.

- CSCud94783

Symptoms: A Cisco ME3600/ME3800 router crashes due to link flaps.

Conditions: This symptom occurs due to link flaps.

Workaround: There is no workaround.

- CSCud94967

Symptoms: OSPF on R-PW gets stuck at exstart/exchange state.

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

Workaround: Remove “ethernet cfm global” configuration to bring up OSPF on R-PW.

- CSCud96075

Symptoms: A router running Cisco IOS Release 15.2(4)M2 will reload with a bus error soon after the DSP reloads when there is a live transcoding session.

Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M2.

Workaround: There is no workaround.

- CSCud99911

Symptoms: There may be a delay of 15 seconds or more before switching over to a backup pseudowire in a pseudowire redundancy configuration.

Conditions: This symptom is observed on the Cisco ME 3600 platform when the attachment circuit is a VLAN.

Workaround: There is no workaround.
- CSCue01579

Symptoms: Receivers on slot10 - 13 of the Cisco 7613 chassis cannot receive multicast traffic when the egress replication mode is used.

Conditions: This symptom occurs on RSP720-10G + CISCO7613 chassis and when using the egress replication mode.

Workaround: Change the replication mode to ingress by using the below given CLI:

mls ip multicast replication-mode ingress
- CSCue01649

Symptoms: CPU errors are seen with (*, G/M) entries on ACL.

Conditions: This symptom is seen on ME3600CX boxes operating in Mode 3 or Mode 4.

Workaround: Operate the ME3600CX boxes in Mode 2.
- CSCue03316

Symptoms: The box crashed during scale testing.

Conditions: During scale testing, the box runs out of memory resulting in MALLOCFAIL. Memory malled is not checked for failure resulting in crash.

Workaround: There is no workaround.
- CSCue03415

Symptoms: Remote CFM MEPs are not discovered with the command “show ethernet cfm maintenance-points remote”. CFM packet debug also does not show any received CCMs even though it is sent correctly from the other end.

Conditions: This symptom is seen when we have UP MEP on EVC-BD with VPLS L2 VFI in the core. The issue occurs in Cisco IOS Release 15.2(2)S2 and later releases.

Workaround: Downgrade to Cisco IOS Release 15.2(1)S2 or lower.
- CSCue03598

Symptoms: Carrier-delay does not work on an ES+ card under the following specific condition:

Carrier-delay configured on gig 4/13 does not work on an ES+ card when you shut down gig0/1 on the peer Cisco 3560 in the below situation:

```

gig4/3[no sh]    gig0/1[no sh]
7600 ===== 3560
gig4/13[sh]     gig0/2[no sh]

```

 1. Do a **no shut** on gig 4/13.
 2. Do a **shut** on gig0/1 right after 1.

gig4/1 will go up as soon as gig 4/3 comes down instead of waiting until the configured carrier-delay timer expires.

Conditions: This symptom occurs when we enter **shut** on the peer device.

Workaround: There is no workaround.

- CSCue05186
Symptoms: FRR LFA will wrongly switch to the alternate path if BFD is unconfigured on the peer router.
Conditions: The symptom is observed if BFD is unconfigured on the peer router.
Workaround: Shut the interfaces with BFD configured, remove the BFD configuration on both routers, then re-enable the interfaces.
- CSCue05358
Symptoms: “Collect Identifier mac-address” -- for routed session is not working for the client who roams to a new interface.
Conditions: This symptom is observed if the subscriber already has a session available in Interface 1.
Workaround: There is no workaround.
- CSCue05844
Symptoms: The Cisco 3925 router running Cisco IOS Release 15.0(2)SG reloads when connecting to a call manager.
Conditions: This symptom is observed with the Cisco 3925 router running Cisco IOS Release 15.0(2)SG.
Workaround: Remove SNMP.
- CSCue05927
Symptoms: OTV ISIS adjacency keeps going down/up every ten minutes.
Conditions: The symptom is observed during normal operation, while IGMP snooping is enabled on switches connected to the routers.
Workaround: Disable IGMP snooping on the switches.
- CSCue06116
Symptoms: VG350 gateway crashes when the configuration file is downloaded from CUCM. This occurs when the VG350 has 144 ports configured.
Conditions: The VG350 supports a maximum of 144 FXS ports. Configure MGCP control and download configuration from CUCM, gateway crashes.
Workaround: Use **no ccm-manager config** to stop the configuration download from CUCM.
- CSCue06383
Symptoms: Classification based on the prec/dscp egress policy does not work as expected.
Conditions: This symptom occurs in L2VPN scenarios when the user has the below given configurations:
 1. DSCP/precedence based policy on egress access EVC of SVI based EoMPLS.
 2. CoS based policy on egress access EVC xconnect.Workaround: There is no workaround.
- CSCue09964
Symptoms: Port based EoMPLS VC is down after flapping the interface. The following steps recreate the issue:
 1. Configure port-based EoMPLS.
 2. Shut the access interfaces. Other side access port will be admin down hence the VC is down. This is expected as per protocol.

3. Now shut the other access interface.
4. Do “no shut” on both the access interfaces, now we expect the VC to come up as per protocol but it does not come up.

Conditions: The symptom is observed on port-based EoMPLS with remote link failure notification feature. It affects the releases from Cisco IOS Release 15.3 onwards.

Workaround: Under the xconnect configuration do **no remote link failure notification**. It will make the VC come up. Then reconfigure the remote link failure notification feature.

- CSCue10844

Symptoms: Classification does not work properly.

Conditions: This symptom occurs only if we have classes based on ACL match and normal DSCP match. Only ACL class will classify properly and other classes do not work.

Workaround: There is no known workaround.

- CSCue15092

Symptoms: A CPU hog is seen at `nile_mgr_bdomain_get_efp_count` and is followed by a crash.

Conditions: This symptom occurs on booting the router with some tunnel configurations.

Workaround: There is no workaround.

- CSCue21993

Symptoms: On a Cisco ME 3600/ME 3800, OSPF sessions flap or go down. Flaps are seen when OSPF is configured on both the interface VLAN and routed ports.

Conditions: The symptom is observed when high rate (18,000 PPS) PIM packets are sent. This issue will be seen with any packets which go on Mcast queue 7, for example: IGMP joins, query.

Workaround: If the high rate PIM/mcast packets is coming from an interface where Mcast traffic can be controlled, configuring COPP will serve as workaround, otherwise, there is no workaround.

- CSCue26213

Symptoms: The connected interface that is enabled for EIGRP will not be redistributed into BGP.

Conditions: This symptom occurs when the prefix of the connected interface is in the EIGRP topology table with “redistribute eigrp” under BGP address-family IPv4.

Workaround: Redistribute the connected interface and EIGRP.

- CSCue27698

Symptoms: Configuring long list of REP block port preferred VLAN will result in losing part of this configuration after the reload.

Example: Configuration like this:

```
rep block port preferred vlan
76-86,94,98,200-201,400,592-593,606-607,611,633,635-636,638,640,643,901-902,1026,
1539,2007-2064
```

will result in two lines in running configuration:

```
rep block port preferred vlan 76-86,94,98,200-201,400,592-593,606-607,611,633
rep block port preferred vlan 635-636,638,640,643,901-902,1026,1539,2007-2064
```

after the reload second line will overwrite the first and only one line will remain:

```
rep block port preferred vlan 635-636,638,640,643,901-902,1026,1539,2007-2064
```

Conditions: This symptom is observed after the reload.

Workaround: Reconfigure the REP block list after the reload.

- CSCue28761
Symptoms: The ISG box crashes when a specific policy-map rule is applied.
Conditions: This symptom occurs when a “default-exit” action is being configured for a regular session.
Workaround: Do not configure the “default-exit” action for regular sessions as it is not a valid action for regular sessions.
- CSCue30237
Symptoms: CFM trace route fails.
Conditions: This symptom occurs in CFM with VPLS in the core. Configure the Up MEP on BD which has the VFI terminated.
Workaround: There is no workaround. The issue is specific to VPLS in the core and Up MEP on the same BD.
- CSCue30590
Symptoms: Packet loss are seen over pseudowire and high CPU.
Conditions: This symptom is observed when IPv6 site-local multicast MAC traffic is sent over SVI EoMPLS, the traffic is looped between the PE of the EoMPLS.
Workaround: There is no workaround.
- CSCue31321
Symptoms: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.
Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.
Workaround: Set “term len 0” before running the **how ip cef ... detail** command.
- CSCue32450
Symptoms: Filtering based on L4 ports does not happen for redirection to CE.
Conditions: This symptom occurs when the WCCP service uses a redirect-list and this ACL has its first entry as a “deny”.
Workaround: Make the first entry in the redirect-list ACL as a “permit”.
- CSCue32596
Symptoms: Targeted LDP session between a Cisco ASR 1000 router and third-party vendor router goes down even though NSR is configured on the Cisco ASR 1000.
Conditions: The symptom is observed when an RP switchover is done on the Cisco ASR 1000, the tLDP session between Cisco ASR 1000 and third-party router goes down.
Workaround: There is no workaround.
- CSCue36197
Symptoms: The Cisco 7600 router may crash while performing the NSF IETF helper function for a neighbor over a sham-link undergoing NSF restart.
Conditions: This symptom occurs when a router is configured as an MPLS VPN PE router with OSPF as PE-CE protocol. OSPF in VRF is configured with a sham-link and a neighbor router over a sham-link is capable of performing an NSF IETF restart on sham-links.
Note: This problem cannot be seen if both routers on sham-link ends are Cisco IOS routers.

Workaround: Disable the IETF Helper Mode protocol by entering the following commands:

```
enable
configure terminal
router ospf process-id [vrf vpn-name]
nsf ietf helper disable
end
```

Note: Disabling Helper Mode will result in an OSPF peer dropping adjacency if the peer is reloaded.

- CSCue36321
Symptoms: A crash occurs when MLP is configured.
Conditions: This symptom is observed with an MLP configuration.
Workaround: There is no workaround.
- CSCue39206
Symptoms: ES crashes after the second 401 challenge.
Conditions: This symptom occurs when the second 401 is received after SDP offer/answer with 183/PRACK is complete. This is a rare scenario.
Workaround: There is no workaround.
- CSCue40354
Symptoms: CPUHOG error message is seen at nile_mgr_bdomain_get_efp_count and then followed by a crash.
Conditions: This symptom is observed on booting the router with scaled mVPN configurations.
Workaround: There is no workaround.
- CSCue43050
Symptoms: VLAN-RAM is programmed with VPN 0. PIM neighborships of random sessions (10-12 out of 30) go DOWN.
Conditions: This symptom occurs when MVPN is configured with 30 L3VPN sessions. When there is a boot up, PIM neighborships of random sessions (10-12 out of 30) go DOWN.
Workaround: Remove and add the VRF configuration for these MVPN sessions.
- CSCue44554
Symptoms: Traffic stops forwarding over port-channels configured with FAST LACP after an RP switch over.
Conditions: This symptom occurs after an RP fail over.
Workaround: A shut/no shut interface will help recover.
- CSCue46302
Symptoms: TAL-failed lite sessions do not convert into dedicated sessions.
Conditions: This symptom occurs when VRF is applied on the access interface.
Workaround: There is no workaround.
- CSCue46590
Symptoms: HTTP POST messages may not be fixed properly after adding scansafe headers.
Conditions: This symptom was first identified on a Cisco ISR running a Cisco IOS Release 15.2(4)M2 image. A Cisco IOS Release 15.2(4)M1 image does not show the problem.
Workaround: Whitelist the domain from being sent over to the towers.

- CSCue46685
Symptoms: Client MAC/framed IP missing in the coa:session query response from ISG.
Conditions: The symptom is observed when you do a COA account-query for lite-session.
Workaround: There is no workaround.
- CSCue51886
Symptoms: The SBC CUBE device rejects call connections.
Conditions: This symptom is observed when the Chunkmanager holds a lot of memory and calls do not get processed.
Workaround: Reloading the box helps to make the box stable.
- CSCue59189
Symptoms: Cisco ME-3600X-24FS-M switch drops R-APS PDU packets and the following error messages are seen in the debug:

```
ERR: Packet with wrong version 0 or opcode 40  
Failed to decode packet, Invalid argument
```


Conditions: The symptom is observed when used with devices that support only G.8032 (2008) for ERPS.
Workaround: There is no workaround.
- CSCue59773
Symptoms: ARP for default gateway will not be resolved
Conditions: This symptom is observed when client has a lite session in ISG and clears the ARP table and then tries to query for the ARP second time
Workaround: Do not clear the ARP entry in the client.
- CSCue62031
Symptoms: A Cisco ME 3600/ME 3800 series switch may reload when a BGP session flaps.
Conditions: This will only be seen if there is more than one BGP neighbor configured on the Cisco ME 3600/ME 3800. It only applies to Cisco IOS Release 15.3(1)S.
Workaround: There is no workaround.
Further Problem Description: This issue is not present in Cisco IOS Release 15.2(2)S.
- CSCue67751
Symptoms: The classification based on QoS group egress policy is not working correctly.
Conditions: With L3VPN configuration, the core interface packets should be classified based on EXP and marked with QoS-group. On the egress interface packets should be classified based on QoS group on the service instance.
Workaround: There is no workaround.
- CSCue76102
Symptoms: Redistributed internal IPv6 routes from v6 IGP into BGP are not learned by the BGP neighboring routers.
Conditions: This symptom occurs because of a software issue, due to which the internal IPv6 redistributed routes from IGPs into BGP are not advertised correctly to the neighboring routers, resulting in the neighbors dropping these IPv6 BGP updates in inbound update processing. The result is that the peering routers do not have any such IPv6 routes in BGP tables from their neighbors.

Workaround: There is no workaround.

- CSCue77909

Symptoms: The interface link shows UP, without fiber IN.

Conditions: This symptom is observed with OCP vendor 100FX SFP on whales2.

Workaround: There is no workaround.

- CSCue78975

Symptoms: Cisco ASR 1000 crashes.

Conditions: There are multiple conditions/scenarios. The issue is observed with the add-path feature on a Release 12 device.

1. Router with version Rel. 12 and above.
2. Configured tags (anywhere in topology) received by Rel. 12 (or above) router.
3. Query received for the route updated with tags earlier.

On the Rel. 12 version device, while freeing routes, a crash is observed. Note: version is an EIGRP release version.

Workaround: There is no workaround.

- CSCue87728

Symptoms: IPv6 traffic is dropped on an egress PE if mLDP is used in the core and the originating PE is a device running anything but IOS.

Conditions: The symptom is observed if mLDP is used in the core and the originating PE is a device running anything but IOS.

Workaround: There is no workaround.

Further Problem Description: Currently on an egress PE, for IPv6 traffic, mLDP only programs the EOS path with link type as IPv6 and there is no NEOS path programmed. Packets are not received with an additional IPv6 explicit null label. However, for inter-op with other vendors, XR adds an IPv6 explicit null label in addition to outer mLDP label when it sends out the packet. Hence, if ingress is XR and egress is IOS then IOS receives packets with explicit null label (at the bottom) and it drops it since there is no NEOS chain.

- CSCue92705

Symptoms: The “DHCPD Receive”, “CDP Protocol”, and “Net Background” processes leaks could be seen after disabling “macro auto monitor”.

Conditions: This symptom is observed in Cisco IOS 15.0(2)SE1 Release, 2960S, dhcp, cdp traffic, and link flapping.

Workaround: Configure “no service dhcp” if the switch is not a DHCP server. Configure:

```
device-sensor filter-spec cdp exclude all
device-sensor filter-spec dhcp exclude all
device-sensor filter-spec lldp exclude all
```

- CSCue94610

Symptoms: DSP crash with the following console error:

```
%SPA_DSPRM-3-DSPALARMINFO: Checksum Failure:80000000,0000000e,d0156a80,d0156000
*Mar 14 17:56:05.851: %SPA_DSPRM-3-DSPALARM: Received alarm indication from dsp
(1/3/6).
%SPA_DSPRM-3-DSPALARMINFO: 0042 0000 0080 0000 0000 0000 4368 6563 6B73 756D
2046 6169 6C75 7265 3A38 3030 3030 302C 3030 3030 3030 3065 2C64 3031 3536
6138 302C 6430 3135 3630 3030 0000 0000 0000 0000 0000
```

Conditions: Error occurs during an RP switchover process. The standby RP presents DSPs failing to come up.

Workaround: This command may clear up the DSPs:

```
Router# hw-module subslot x/y reload...
```

- CSCue97986

Symptoms: Calls hang at SIP, CCAPI and VOIP RTP components (but are cleared in the dataplane of the Cisco ASR 1000 series platform).

Conditions: This symptom occurs when a video call is setup as an audio call. The call then gets transferred with REFER but the caller hangs up the call before the call gets transferred. This is an intermittent problem.

Workaround: If there is an SIP call dangling (sh sip call sum), then use the “clear cal voice causecode 16” command to clear the dangling call.

- CSCuf01088

Symptoms: Memory leaks are observed with a Cisco ASR router with CVP call flows.

Conditions: The symptom is observed under load conditions. Memory leaks are seen in Cisco IOS XE 3.8.

Workaround: There is no workaround.

- CSCuf04674

Symptoms: Standby continuously crashes with traceback on pm_vlan_deallocate.

Conditions: The symptom is observed when the router has both active and standby. When the router is coming up, the standby is crashing continuously though the active comes up without any issues. The router has an MDT configuration.

Workaround: There is no workaround.

- CSCuf15260

Symptoms: A Cisco ASR router crashes while sending notify with KPML digit.

Conditions: The symptom is observed on a Cisco ASR router. It is seen when the DTMF type is changing to SIP-KPML midcall.

Workaround: Do not change DTMF type mid-call.

- CSCuf16504

Symptoms: Classification based on the QoS group along with prec/dscp at the egress policy does not function as expected.

Conditions: This symptom occurs with L2VPN/L3VPN configuration. On the core interface, packets should be classified based on exp and marked with the QoS group. On the egress interface, packets should be classified based on the QoS group and prec/dscp/cos inner.

Workaround: There is no workaround.

- CSCuf17009

Symptoms: With PIM enabled on a P2P GRE tunnel or IPsec tunnel, the SP of the Cisco 7600 series router might crash.

Conditions: This symptom occurs when there are more number of tunnels going via the same physical interface. This issue is seen in Cisco IOS SREx and Cisco IOS 15.S based releases only.

Workaround: There is no workaround.

- CSCuf20407
Symptoms: Tracebacks are seen on ME3600X-24CX-M bootup.
Conditions: This symptom occurs when ME3600X-24CX-M boots with Cisco IOS Release 15.2(4)S0.2, Cisco IOS Release 15.3(1)S0.1 or prior releases on the new Rev 2 HW.
Workaround: There is no workaround.
- CSCuf20537
Symptoms: The router crashes due to null pointer dereference.
Conditions: This symptom occurs with the C4 VSS system (2 sup vss) with dual-homed fex stack (This has not been seen on other platforms, but the fix is ported as a precautionary measure). During the first SSO, no crash is observed [Active and Standby (Hot-Standby)]. During the second SSO, a crash is observed.
Workaround: There is no workaround.
- CSCuf25555
Symptoms: Policy-based routing stops working after the router reloads.
Conditions: This symptom occurs when multiple next-hops configured on the same route map are reachable through the same interface.
Workaround: Remove and reconfigure the route-map.
Further Problem Description: This is a specific scenario where multiple next-hops configured on the same route map are reachable through the same physical interface on different VLANs.
After reload, when the physical interface comes up, adjacency for all configured next-hops on different sequence numbers of the same route map were notified to the PD client simultaneously.
- CSCuf65724
Symptoms: LISP control packets dropped in the network.
Conditions: The symptom is observed when there are more than 32 hops between sender and receiver.
Workaround: There is no workaround.
Further Problem Description: LISP control packets are sent with an IP TTL of 32, meaning if there is more than 32 IP hops between the sender and receiver, they will be dropped in the network.

Resolved Bugs—Cisco IOS Release 15.3(1)S1

Cisco IOS Release 15.3(1)S1 is a rebuild release for Cisco IOS Release 15.3(1)S. The bugs in this section are resolved in Cisco IOS Release 15.3(1)S1 but may be open in previous Cisco IOS releases.

- CSCtc42734
Symptoms: A communication failure may occur due to a stale next-hop.
Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.
Workaround: Reload the router.
- CSCtg82170
Symptoms: The IP SLA destination IP/port configuration changes over a random period of time. This issue is hard to reproduce but has been reported after upgrading to Cisco IOS Release 15.1(1)T.

So far, it only seems to have affected the destination IP and port. The destination IP may be changed to an existing destination IP that has already been used by another probe. The destination port is sometimes changed to 1967 which is reserved for IP SLA control packets. Other random destination ports have also been observed to replace the configured port for some of the IP SLA probes. Each time when the change happens, many of the IP SLA probes will stop running.

Conditions: This symptom is observed in Cisco IOS Release 15.1(1)T. Other Cisco IOS versions may also be affected.

Workaround: There is no workaround.

- CSCtj89743

Symptoms: The Cisco Catalyst 4000 series switches running Cisco IOS Release 12.2(54)SG experiences high CPU when issuing an unsupported command, **https://ip-address**, in which ip-address is accessible from this device.

Conditions: This symptom is observed with the Cisco Catalyst 4000 series switches.

Workaround: There is no workaround.

Further Problem Description: Even if SSL handshake fails, the HTTP CORE process is looping and is scheduled repeatedly.

- CSCts75737

Symptoms: Tracebacks are seen at swidb_if_index_link_identity on the standby RP.

Conditions: This symptom is observed when unconfiguring and reconfiguring “ipv4 proxy-etr” under the router LISP.

Workaround: There is no workaround.

- CSCtw65575

Symptoms: The router may unexpectedly reload when OSPFv3 MIB is polled via SNMP.

Conditions: This symptom occurs when OSPFv3 is configured with area ranges whose prefix length is /128. A router with no area ranges is not vulnerable.

Workaround: Configure area ranges to have a smaller prefix length (that is, in the range of /0 to /127).

- CSCtx31177

Symptoms: RP crash is observed on avl_search in a high scaled scenario.

Conditions: This symptom is observed in a high scaled scenario with continuous traffic flow.

Workaround: There is no workaround.

- CSCtx36095

Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

Conditions: This symptom occurs during a line card reload.

Workaround: There is no workaround.

- CSCty44654

Symptoms: The router crashes when trying to test the MVPN6 functionality.

Conditions: This symptom is observed with the following conditions:

- Configure the router to test the MVPN6 functionality.
- Delete the VRF associated with the interface in the MVPN6 test configuration.

Workaround: There is no workaround.

- CSCty57476
Symptoms: The BGP GSHUT feature needs to add support for the AA:NN format for community.
Conditions: This symptom is observed when support is added for the AA:NN format for community when using the BGP GSHUT feature.
Workaround: The <1-4294967295> community number can be used instead of the AA:NN format.
- CSCtz55979
Symptoms: The router crashes.
Conditions: This symptom occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.
Workaround: There is no workaround.
- CSCua20373
Symptoms: After SSO, all the GRE tunnels get admin down and stay down until the security module SSC-600/WS-IPSEC-3 comes up. Complete traffic loss is seen during this time.
Conditions: This symptom is observed when Vanilla GRE tunnels are configured in the system where HA and the IPsec Module SSC-600/WS-IPSEC-3 card is present, “crypto engine mode vrf” is configured, and SSO is issued.
Workaround: Remove the “crypto engine mode vrf” configuration if IPsec is not enabled on the router.
- CSCua61330
Symptoms: Traffic loss is observed during switchover if,
 1. BGP graceful restart is enabled.
 2. The next-hop is learned by BGP.Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.
Workaround: There is no workaround.
- CSCua75069
Symptoms: BGP sometimes fails to send an update or a withdraw to an iBGP peer (missing update)
Conditions: This symptom is observed only when all of the following conditions are met:
 1. BGP advertise-best-external is configured, or diverse-path is configured for at least one neighbor.
 2. The router has one more BGP peers.
 3. The router receives an update from a peer, which changes an attribute on the backup path/repair path in a way which does not cause that path to become the best path.
 4. The best path for the net in step #3 does not get updated.
 5. At least one of the following occurs:
 - A subsequent configuration change would cause the net to be advertised or withdrawn.
 - Dampening would cause the net to be withdrawn.
 - SOO policy would cause the net to be withdrawn.
 - Split Horizon or Loop Detection would cause the net to be withdrawn.
 - IPv4 AF-based filtering would cause the net to be withdrawn.
 - ORF-based filtering would cause the net to be withdrawn.

- The net would be withdrawn because it is no longer in the RIB.

The following Cisco IOS releases are known to be impacted if they do not include this fix:

- Cisco IOS Release 15.2T and later releases
- Cisco IOS Release 15.1S and later releases
- Cisco IOS Release 15.2M and later releases
- Cisco IOS Release 15.0EX and later releases

Older releases on these trains are not impacted.

Workaround: If this issue is triggered by a configuration change, you can subsequently issue the **clear ip bgp neighbor soft out** command.

- CSCua96354

Symptoms: Reload may occur when issuing the **show oer** and **show pfr** commands.

Conditions: This symptom is observed with the following commands:

- **show oer master traffic-class performance**
- **show pfr master traffic-class performance**

Workaround: There is no workaround.

- CSCub04982

Symptoms: In an IPFRR configuration, a traceback is seen about changing the FRR primary OCE where the new OCE has a different interface and next-hop, which blocks such a linkage.

Conditions: This symptom occurs while changing the FRR primary OCE interface to a new OCE with a different interface.

Workaround: There is no workaround.

- CSCub23231

Symptoms: Very specific events/packet types cause the ES20 LC to stop passing traffic. Information on these events and packets that lead to the issue are not known currently.

Conditions: This symptom occurs when the ES20 interface has an EVC or MPLS configuration.

Workaround: Reload LC.

- CSCub68933

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

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

Workaround: There is no workaround.

- CSCub74272

Symptoms: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then the VTI tunnel line protocol goes down.

Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T, with VTI over GRE.

Workaround: There is no workaround.

- CSCub78299

Symptoms: Ping fails from host1 (192.168.1.2) to host2 (192.168.4.2).

Conditions: This symptom occurs when Suite-B is configured on IPsec sa.

Workaround: There is no workaround.

- CSCub80386

Symptoms: The following interface configuration should be used:

```
interface Ethernet2/1
description lanethernet1
ipv6 enable
ospfv3 100 network manet
ospfv3 100 ipv6 area 0
```

Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval** command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80710

Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

Workaround: There is no workaround.

- CSCub85451

Symptoms: When ScanSafe is enabled on the interface, latency may be seen. Some pages may not load at all or show severe latency if the SYN request sent by the ISR does not receive an appropriate SYN ACK response from the ScanSafe Tower.

Conditions: ScanSafe must be enabled on the interface. In this case, there was an ASA in the path that was doing sequence number randomization.

Workaround: Disable sequence number randomization on the firewall in the path before the ISR.

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 4.3/4.1:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C> CVE ID CVE-2012-4651 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

- CSCub87579

Symptoms: Multicast traffic gets forwarded to the wrong tunnel protected with IPsec.

Conditions: This symptom is observed when Multicast (PIM) is enabled on the GRE tunnel protected with IPsec on the Cisco 7600.

Workaround: Shut/no shut on the tunnel protected with IPsec resolves the issue.

- CSCub89144

Symptoms: The VTI tunnel is always in up/up state.

Conditions: This symptom is observed when HSRP failover is configured on the HSRP standby router only. This issue was first seen on the Cisco ASR router, but it is platform-independent and is seen on the latest Cisco IOS Release 15M&T and later releases as well.

Workaround: Use GRE or routing protocols for redundancy.

- CSCuc05570

Symptoms: The “PM-SP-STDBY-3-INTERNALERROR” error message is seen on Active for the Tunnel Reserved VLAN and the Tunnel Global Reserved VLAN.

Conditions: This symptom is observed with an HA router with a scale configuration of the MDT Tunnel.

Workaround: There is no workaround.

- CSCuc08061

Symptoms: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

Workaround: Reboot the spoke.

- CSCuc13992

Symptoms: The Cisco IOSd process crashes due to a segmentation fault in the PPP process:

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events
```

The root cause for the PPP process crash is wrong IPCP option processing inside PPP control packets.

Conditions: This symptom occurs when the BRAS functionality is configured, which includes ISG and PPPoE session termination.

Workaround: There is no workaround.

- CSCuc19046

Symptoms: Active Cisco IOSd was found to have crashed following the “clear ip mroute *” CLI.

Conditions: This symptom occurs with 4K mroutes (2k *,G and 2K S,G) running the FFM performance test suite.

Workaround: There is no workaround.

Further Problem Description: So far, this issue is only seen in the FFM performance test script.

- CSCuc32119

Symptoms: Traffic drop is seen due to misprogramming in the VLAN RAM table.

Conditions: This symptom is observed when the router is reloaded multiple times.

Workaround: There is no workaround.

- CSCuc34304

Symptoms: A crash is seen in pim_reg_enc_src_update_mvrf in complex multicast setup.

Conditions: This symptom is seen when traffic is active for a combination of different IPv4 multicast VPN features/scenarios. Cisco IOS may crash upon interface coming up notification.

Workaround: There is no workaround.

- CSCuc36469

Symptoms: Crash is observed when removing the **crypto call admission limit ike in-negotiation-sa** *value* configuration and clear crypto sessions, which triggers a connection from all the clients burdening the server and forcing it to crash within seconds.

Conditions: This symptom happens only when 150 connections simultaneously try to establish connection with the head-end EzVPN server.

Workaround: Configure **crypto call admission limit ike in-negotiation- sa 20** when scaling to 150 tunnels.
- CSCuc37047

Symptoms: VSS crashes on reconfiguring “ipv6 unicast-forwarding” multiple times.

Conditions: This symptom occurs when CTS is configured on an interface and “ipv6 unicast” is toggled multiple times.

Workaround: There is no workaround.
- CSCuc44629

Symptoms: The switch/router crashes while processing NTP.

Conditions: This symptom occurs if NTP is configured using DNS, along with the source interface. For example: `config# ntp server dns source interface`

Workaround 1: `config# ntp server dns`

Workaround 2: `config# ntp server ip`

Workaround 3: `config# ntp server ip source interface`

For workarounds 1 and 2, the device automatically selects the source interface. For workarounds 2 and 3, resolve the DNS and use the corresponding IP address for that DNS. For example: `Router# ping dns`.

The above command gives the IP address for DNS. Use that IP address to configure the NTP server.
- CSCuc45115

Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at `nhrp_add_static_map`.

Conditions: This symptom is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

Workaround: There is no known workaround.
- CSCuc48162

Symptoms: EVC Xconnect UP MEP is sending CCMs when the remote EFP is shut.

Conditions: This symptom occurs when EFP is admin down.

Workaround: There is no workaround.
- CSCuc48211

Symptoms: Traffic from the Label Edge Router (LER) is dropped at the Label Switch Router (LSR) peer. LER is using a invalid/outdated label, unknown to LSR. This issue can be seen with a regular MPLS connection over a physical interface or with a connection over an MPLS TE tunnel interface. The root cause is that LER is using CEF long-path extension, installed to the prefix by a different routing protocol in the past.

```
TUNNEL-HEADEND/LER#show ip cef 172.25.0.1 internal
```

```

172.25.0.0/16, epoch 6, flags rib only nolabel, rib defined all labels, RIB[B],
refcount 5, per-destination sharing
sources: RIB
feature space:
  IPRM: 0x00018000
  Broker: linked, distributed at 4th priority
  LFD: 172.25.0.0/16 0 local labels
      contains path extension list
ifnums:
  TenGigabitEthernet1/0/0(31): 10.10.243.48
  Tunnel11(38)
  path 1F13EC1C, path list 1436FC80, share 1/1, type recursive, for IPv4
  recursive via 10.10.254.3[IPv4:Default], fib 21B2A5CC, 1 terminal fib,
v4:Default:10.10.254.3/32
  path 13A71668, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
  MPLS short path extensions: MOI flags = 0x1 label 1683
  nexthop 10.10.243.48 TenGigabitEthernet1/0/0 label 1683, adjacency IP adj
out of TenGigabitEthernet1/0/0, addr 95.10.243.48 20BCED00
  path 13A745A8, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
  MPLS short path extensions: MOI flags = 0x1 label 623
  MPLS long path extensions: MOI flags = 0x1 label 18
  nexthop 10.10.255.130 Tunnel11 label 18, adjacency IP midchain out of
Tunnel11 22923160
  long extension for path if Tunnel11 next hop 10.10.255.130:
  MPLS long path extensions: MOI flags = 0x1 label 18
  long extension for path if Tunnel22 next hop 10.10.255.129:
  MPLS long path extensions: MOI flags = 0x1 label 651
output chain:
  loadinfo 212F8810, per-session, 2 choices, flags 0083, 4 locks
  flags: Per-session, for-rx-IPv4, 2buckets
  2 hash buckets
    < 0 > label 1683 TAG adj out of TenGigabitEthernet1/0/0, addr
10.10.243.48 20BDC860
    < 1 > label 18 TAG midchain out of Tunnel11 20C92B00 label implicit-null
TAG adj out of TenGigabitEthernet1/0/1, addr 10.10.243.50 20B21440
Subblocks:
  None

```

```

TUNNEL-TAILEND/LSR# sh mpls forwarding-table labels 18
Local      Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label      Label     or Tunnel Id   Switched     interface
TUNNEL-TAILEND#

```

Conditions: This symptom occurs when the prefix is learned by both BGP and IGP, while BGP has lower Administrative Distance, pointing via the MPLS TE tunnel carrying MPLS. This issue is seen once the prefix is installed to RIB by IGP and then by BGP (Reload, BGP flap, etc.); then, the CEF will keep using the IGP/LDPs label without updating it in case of LDP label change.

Workaround: Issue the **clear ip route prefix mask** command.

- CSCuc53135

Symptoms: LDP sessions are not established.

Conditions: This symptom is observed on a router with more than one LDP adjacency to a neighbor. This issue is seen when the TCP session establishment to that neighbor is delayed, and while it is delayed, the adjacency that is the active adjacency times out (no more UDP packets are received), resulting in the TCP listen socket being deleted and not created.

Workaround: Issue the **clear mpls ldp neighbor *** command.

- CSCuc55346

Symptoms: SNMP MIB cbQosCMDropPkt and cbQosCMDropByte report 0.

Conditions: This symptom is observed with Cisco IOS Release 15.1(3)S1 and Cisco IOS Release 15.2. This issue is not seen with Cisco IOS Release SRE4.

Workaround: Use SNMP MIB `cbQosPoliceExceededPkt` and `cbQosPoliceExceededByte`.

- CSCuc55634

Symptoms: IPv6 static route cannot resolve the destination.

Conditions:

1. A VRF is configured by the old style CLI (for example “ip vrf RED”).
2. Configure “ip vrf forwarding RED” under an interface.
3. Configure IPv6 address under the same interface (for example 2001:192:44:1::2/64).
4. Configure IPv6 static route via the interface configured in item 3, (for example IPv6 route 2001:192:14:1::/64 2001:192:44:1::1).
5. Then, we are not able to ping the “2001:192:14:1::2” although we can reach to “2001:192:44:1::1”.

Workaround: There is no workaround.

- CSCuc56259

Symptoms: A Cisco 3945 that is running Cisco IOS Release 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

```
%VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times
and
```

```
Delivery Ack could not be sent due to lack of buffers.
```

Conditions: This happens when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc59049

Symptoms: The Cisco ME3800x crashinfo files may be incomplete.

Conditions: This symptom occurs when a crashinfo file is created when a crash occurs.

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

- CSCuc59105

Symptoms: The switch may crash when issuing “show platform qos policer cpu x x”.

Conditions: This symptom occurs only when issuing “show platform qos policer cpu x x” through an SSH session.

Workaround: Execute the command through Telnet or the console.

- CSCuc59765

Symptoms: Cisco ME 380x and ME 360x fail to trigger watchdog crash in certain scenarios.

Conditions: This symptom is seen when soaking over a prolonged period of time.

Workaround: There is no workaround.

- CSCuc60245

Symptoms: Pseudowires stop passing traffic until the LSP is reoptimized.

Conditions: This symptom is observed when pseudowires stop passing traffic until the LSP is reoptimized.

Workaround: The common fix is reoptimizing the LSP onto a new path in one or both directions.

- CSCuc63531

Symptoms: The following traceback may be displayed after performing Stateful Switchover:

```
%SYS-2-NOBLOCK: may_suspend with blocking disabled.
```

Conditions: This symptom is observed when Stateful Switchover is performed with the **template type pseudowire** command configured.

Workaround: There is no workaround.

- CSCuc64899

Symptoms: The router does not learn remote Connectivity Fault Management (CFM) Maintenance Endpoint (MEPs).

Conditions: This symptom occurs on interfaces with an xconnect statement after a reload on a peer device.

Workaround: Remove and re-apply the CFM configuration.

- CSCuc65424

Symptoms: On dual RP configurations, a standby route processor might crash when establishing new interfaces (could be PPP sessions).

Conditions: This symptom is observed when IDB reuse is turned on on a dual RP configuration, and when some interfaces are deleted and created again.

Workaround: Turn off the IDB reuse option.

- CSCuc66122

Symptoms: A crash occurs with the **show ip sla summary** command with the IP SLAs RTP-Based VoIP Operation.

Conditions: This symptom occurs when the IP SLAs RTP-Based VoIP Operation is configured on the box.

Workaround: Use the **show ip sla statistics** command to check the status and statistics of the IP SLAs RTP-Based VoIP Operation rather than **show ip sla summary** command, when the IP SLAs RTP-Based VoIP Operation is configured on the box.

- CSCuc70310

Symptoms: RRI routes are not installed in DMAP. “Reverse-route” is a configuration in the DMAP. This prevents packets from being routed through the intended interface, and hence packet loss occurs.

Conditions: This symptom is observed when a simple reverse-route is configured in DMAP without any gateway options.

Workaround: There is no workaround.

- CSCuc71493

Symptoms: Significant transaction time degradation is observed when an e-mail with attachment(s) is sent from the Windows 7 client using Outlook to a server running Outlook 2010 on the Windows 2008 server and the WAN latency is low, that is, ~12ms RTT.

Conditions: This symptom is observed when the client is Windows 7 and data is being uploaded using the MAPI protocol and the connection is being optimized by WAAS-Express.

Workaround: Disable WAAS-Express.

- CSCuc72244

Symptoms: On the Cisco 7600, both sides running Cisco IOS Release SRE4, Ethernet SPA configured with “negotiation Auto” and changed to “no negotiation auto”. The interface is operating in half-duplex instead of full-duplex mode.

Conditions: This is a timing issue seen when configuring/un-configuring auto-negotiation or when doing continuous router reload.

Recovery action: Configuring “shut” and “no shut” on the interface changes the duplex state to full-duplex.

Workaround: There is no workaround.
- CSCuc73677

Symptoms: RSA keys are not generated correctly.

Conditions: This symptom occurs when you first clear the RSA keys that are already generated on the router, and then generate the RSA keys.

Workaround: There is no workaround.
- CSCuc76130

Symptoms: IPsec SAs are not getting deleted even after removing ACL.

Conditions: This symptom occurs when using the IPsec feature with Cisco IOS Release 15.3(0.18)T0.1.

Workaround: There is no workaround.
- CSCuc76515

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

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

Workaround: Clear xconnect peer.
- CSCuc77283

Symptoms: Upon reload or OIR, the CFM MEP configuration on an xconnect EFP is removed and cannot be reconfigured.

Conditions: This symptom is observed with a CFM MEP on xconnect service instance. This issue is seen when reload or OIR is performed.

Workaround: Remove the domain configuration.
- CSCuc77704

Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

 - esp-sha256-hmac
 - esp-sha384-hmac
 - esp-sha512-hmac

Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc79161

Symptoms: Memory leak is observed.

Conditions: This symptom occurs after flapping the interface, keeping the setup idle, and executing “clear xconnect”.

Workaround: There is no workaround.

Further Problem Description: The PI front-end pseudoport is not deleted when the xconnect is removed, which causes the memory leak. This issue occurs because PD returns BDOMAIN_PP_FAILED to PI when pp_engine_context is a NULL pointer.
- CSCuc79923

Symptoms: On a Cisco 7600 running Cisco IOS Release 15.2(4)S1, packets from FWSM are dropped when the servicemodule session is enabled. Ping fails for the VLAN interface on the FWSM module from the supervisor. The ARP entry is incomplete on the Cisco 7600.

Conditions: This symptom is observed with the following conditions:

 - This issue is seen on the Cisco 7600 with FWSM and SUP-720-3B running Cisco IOS Release 15.2(4)S1.
 - The FWSM is in Crossbar mode.
 - The system is in “distributed” egress SPAN replication mode.

This issue is not seen with Cisco IOS Release 12.2(33)SRE7.

Workaround:

 - Disable the servicemodule session.
 - Change the fabric switching mode to bus.
 - Change SPAN egress replication mode to “centralized”.
- CSCuc82551

Symptoms: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.

Conditions: This symptom is observed with SNMP polling with an IP SLA configuration.

The crash signature is as follows:

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
```

Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.
- CSCuc88175

Symptoms: When a dynamic cryptomap is used on the Virtual Template interface, SAs do not created and thus the testscripts fail. This issue occurs because the crypto map configurations are not added to the NVGEN, and hence there is no security policy applied on the Virtual Template interface.

Conditions: This symptom occurs only when a dynamic map is used on the Virtual Template interface. However, this issue is not seen when tunnel protection is used on the Virtual Template interface or when a dynamic map is used on the typical physical interface.

Workaround: There is no workaround apart from using tunnel protection on the Virtual Template interface.
- CSCuc88312

Symptoms: A memory leak is seen at cca_realloc_cb_ce_mask.

Conditions: This happens when CCA is configured on multiple interfaces and one of them is brought down.

Workaround: There is no workaround.

- CSCuc90580

Symptoms: Ping fails over RoutedPW.

Conditions: This symptom is seen with SVI based MPLS uplink.

Workaround: Disable mac learning.

- CSCuc93361

Symptoms: “IP” protocol is not accepted in the **ping** command with the IPv6 address configured.

Conditions: This symptom occurs when a single interface is configured with an IP address, and later, the mask alone is changed. For example:

```
int e0/0
ip addr 10.1.1.1 255.255.255.0
no shut
```

Later,

```
int e0/0
ip addr 10.1.1.1 255.255.0.0
```

Workaround: Configure a different IP address and then revert to the same address with the changed mask. For example:

```
int e0/0
ip addr 10.1.1.1 255.255.255.0
no shut
```

Later,

```
int e0/0
ip addr 10.1.1.2 255.255.0.0
ip addr 10.1.1.1 255.255.0.0
```

- CSCuc94983

Symptoms: Node crashes.

Conditions: This symptom is seen with rigorous flapping of the core.

Workaround: Have a stable core network.

- CSCuc96345

Symptoms: ARP exchange between the Cisco 7600 and the client device fails. The Cisco 7600 has an incomplete ARP entry in its ARP table for the client. This issue is likely to be seen between the Cisco 7600 and other Cisco platforms with MAC address 6073.5Cxx.xxxx. The incoming ARP reply is parsed by the platform CEF as an IP packet and dropped.

The following OUIs (as of October 30, 2012) are affected: (first 3 bytes from MAC address/MAC starts with)

14-73-73

20-73-55

4C-73-67

4C-73-A5

54-73-98

60-73-5C (One of Cisco's OUI ranges)

64-73-E2

70-73-CB

8C-73-6E

98-73-C4

A0-73-32

C4-73-1E

D0-73-8E

F0-73-AE

F4-73-CA

Conditions: This symptom is observed with the EVC pseudowire and 802.1q subinterface on the same physical interface, and connectivity via the subinterface is affected.

Sample configuration:

```
interface TenGigabitEthernet3/1 service instance 2013 ethernet encapsulation dot1q 411
second-dot1q 200 rewrite ingress tag pop 2 symmetric xconnect 10.254.10.10 3350075
encapsulation mpls interface TenGigabitEthernet3/1.906 encapsulation dot1Q 906 ip address
10.10.10.1 255.255.255.0
```

Workaround:

- There should be a static ARP entry on the Cisco 7600 for the client's MAC and IP.
- Change the MAC address of client to a nonaffected OUI.

- CSCuc98226

Symptoms: When a PC is moved between two VLAN ports (on one port, ISG is enabled, and the other is non-ISG) several times by its LAN cable connection on the L2SW that is connected to the Cisco ASR 1000 router, the PC becomes unable to acquire an IP address from DHCP on the router. At that time, an incorrect interface is shown in "show ip dhcp binding".

Conditions: This symptom is observed with Cisco IOS Release 15.2(4)S1.

Workaround: There is no workaround.

- CSCud03273

Symptoms: All the paths using certain next-hops under the route-map are marked inaccessible.

Conditions: This symptom occurs under the following conditions:

1. Configure peer groups.
2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).
3. Configure the Prefix-list.
4. Configure the route-map.
5. Configure the BGP neighbor and add them to peer groups.

Workaround: Configure "route-map permit *seq-num name*" or activate at least one neighbor in "address-family ipv4".

- CSCud06237

Symptoms: Local ID is 0.0.0.0 in PfR target discover feature.

Conditions: This symptom is seen when manual EIGRP is used for PfR target discover feature.

Workaround: There is no workaround.

Further Problem Description: A site will not be able to publish its local prefixes.

- CSCud06438
Symptoms: IP sessions do not come up after the DHCP failure is encountered.
Conditions: This symptom occurs when the DHCP address pool is not configured in the DHCP server and if an DHCPDISCOVER request is sent from the client to the server.
Workaround: There is no workaround.
- CSCud06887
Symptoms: IPsec stateful failover is configured between two routers.
router_1 is chosen as Active.
router_2 is chosen as Standby.
router_3 acts as the VPN end peer.
 - A VPN tunnel is created between the VIP of routers 1 and 2 and router_3.
 - SPIs are replicated from Active (router_1) to Standby (router_2).
 - After switchover from Active to Standby (done by reload of Active router_1), router_2 becomes Active and takes over the VPN connection.
 - Router_1 comes up after manual reload and then reloads again by itself.
 - When router_1 comes up after the second reload, SPIs are not replicated from Active router_2.Conditions: This symptom occurs when IPsec stateful failover is configured on Cisco IOS Release 15.2(4)M1. This issue is seen when the HW crypto engine is enabled.
Workaround: There is no workaround. When next switchover from Active to Standby will be triggered, then new VPN connection is being created, packet loss occurs.
- CSCud07642
Symptoms: The ASR 903 is unable to pass traffic to the ASR 9000.
Conditions: Occurs with a clear-channel ATM over MPLS configuration using AAL0 encapsulation.
Workaround: Enable MPLS control-word on the ASR 9000.
- CSCud07856
Symptoms: SP crashes at “cfib_update_ipfrr_lbl_ref_count”.
Conditions: This symptom is observed with a scaled IP-FRR configuration.
Workaround: Remove the IP-FRR configuration.
- CSCud09627
Symptoms: The following error message is seen on the console:

```
npm_intfman_get_el3idc_vlan_index:interface el3id handle is NULL
```

Conditions: This symptom is seen under the following conditions:
 - no mpls traffic-eng tunnels
 - mpls traffic-eng tunnels
 - clear ip bgp *or
 - on doing IM OIR on peer endWorkaround: There is no workaround.

- CSCud16693

Symptoms: The Cisco ME3600X/ME3800X switch crashes as soon as you apply policy-map referencing table-map.

Conditions: This symptom occurs when applying a service policy which has an unsupported combination of police action with table-map and without table-map.

Workaround: Configure a service policy which does not have the combination of police action with table-map and without table-map.
- CSCud17547

Symptoms: Mismatch of mplsXCLspId CLI and SNMP value is observed.

Conditions: This symptom is seen when snmp query is performed.

Workaround: There is no workaround.
- CSCud17934

Symptoms: PW redundancy on the Cisco 7600 does not work when the primary VC goes down and the backup VC takes over, and CE to CE communication is broken.

Conditions: This symptom is observed with the following conditions:

 - The MPLS facing LC is WS-X6704-10GE.
 - The CE facing LC is ES+.

Workaround: Use another HW on the MPLS core.
- CSCud19230

Symptoms: ES+ line card reload occurs with the following error messages:

```
%PM_SCP-SP-1-LCP_FW_ERR: System resetting module 2 to recover from error:
x40g_iofpga_interrupt_handler: LINKFPGA IOFPGA IO Bus Err val: 4214784 Bus Error
Add:332 Bus Err data: 0
%OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled Off (Module Reset due to
exception or user request)
%C7600_PWR-SP-4-DISABLED: power to module in slot 2 set Off (Module Reset due to
exception or user request)
```

Conditions: This symptom is observed with the ES+ line card.

Workaround: There is no workaround.
- CSCud19257

Symptoms: NAT CLIs expose the **vrf** keyword on the Cisco 7600, which is not supported.

Conditions: This symptom is observed with a NAT configuration.

Workaround: Do not use the **vrf** keyword for NATing on the Cisco 7600.
- CSCud22601

Symptoms: MPLS-TP tunnels remain down after the standby RSP boots.

Conditions: Occurs when you boot the standby RSP after applying an MPLS-TP configuration and performing an SSO. The issue occurs rarely.

Workaround: Issue a **shutdown/no shutdown** on the MPLS-TP tunnel. A nonintrusive workaround is to cause a flap on the protect label switched path (LSP) by reconfiguring the path or physically shutting down and restoring the interface.
- CSCud24084

Symptoms: Performing a default MDT toggling on a VRF results in the encapsulation tunnel adjacency's MTU being set to a lower MTU.

Conditions: This symptom is observed with Cisco IOS XE Release 3.7S (Cisco IOS Release 15.2(4)S) and later releases when the `mdt default <>` is toggled on a VRF.

Workaround: Delete and add the affected VRF.

Further Problem Description: Software adjacency does not updated with the correct MTU.

- CSCud26339

Symptoms: Changing policy-map parameters triggers a Cisco IOSd crash.

Conditions: This symptom is observed when the policy-map is attached to a service instance on the Cisco ASR 903.

Workaround: Remove the policy-map from the target and then make the changes.

- CSCud27379

Symptoms: WS-SUP720-3B running Cisco IOS Release 12.2(33)SRE4 crashes at `get_alt_mod` after issuing “`sh run int g4/13`” with several trailing white spaces until the cursor stops moving.

Conditions: This symptom occurs when you issue the **show run interface** command with trailing spaces until the cursor stops moving.

Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud28759

Symptoms: SPA crash is seen when invoking `spa_choc_dsx_cleanup_atlas_ci_config` with no data packed.

Conditions: This symptom is observed when the packed data size should be 1 and the status should be success.

Workaround: There is no workaround.

- CSCud31012

Symptoms: MVPNv6 does not work in the Cisco IOS XE Release 3.7S image.

Conditions: This symptom is observed only with the IP services image.

Workaround: Use the enterprise image.

- CSCud31808

Symptoms: With the two commands configured listed under the conditions of this release note, the Cisco router might start advertising a low TCP receive window size to the TCP peer for a specific TCP transaction. The value of this receive window size becomes equal to the configured MSS value, and it will never exceed this value anymore. This might impact TCP performance.

Conditions: This symptom happens only if the following two commands are configured on the router:

ip tcp mss x

ip tcp path-mtu-discovery

Workaround: Either change the path-mtu discovery ager timeout to 0, or remove one of the two commands.

- CSCud33564

Symptoms: BFD sessions are not offloaded.

Conditions: This symptom occurs when XDR infra creates a split event for an XDR mcast_grp and the BFD client ignores it. For this bug, the reason for the split is that a slot is not able to process messages as fast as other slots, thus causing distribution for all slots to block while it catches up. This issue typically occurs with either of the following conditions:

1. The slot has a slower CPU than the others.
2. The amount of work being done during processing of messages is greater than on other slots.

Workaround: Reload ES+ cards.

- CSCud33887

Symptoms: The 6VPE packets get punted and policed.

Conditions: This symptom is seen when ESP header is enabled.

Workaround: There is no workaround.

- CSCud35423

Symptoms: IOSD crashes on ISG policy handling process.

Conditions: This symptom is seen while handling ISG subscriber traffic.

Workaround: There is no workaround.

- CSCud36113

Symptoms: Ping fails between CE routers.

Conditions: This symptom is observed when you configure MPLS VPN Inter-AS IPv4 BGP Label Distribution and flaps “mpls bgp forwarding” in the interface between ASBRs.

Workaround: Removing and adding (flapping) the static routes between ASBRs resolves the issue.

- CSCud36208

Symptoms: The multilink ID range has to be increased from the existing 65535.

Conditions: This symptom is observed specifically with the Cisco MWR1.

Workaround: There is no workaround. The range is now made configurable based on PD.

- CSCud36723

Symptoms: RPF information for IPv6 multicast mroutes is not updated when routing changes.

Conditions: This symptom occurs when an IPv6 multicast configuration is present in the startup configuration.

Workaround: After startup, remove all IPv6 multicast configurations, if any, and then apply the configuration as needed.

- CSCud58016

Symptoms: DHCP clients are not allocated IP address.

Conditions: This symptom occurs when default session is configured on the interface and DHCP discover is received on that interface.

Workaround: Keep the DHCP and walkby sessions on different interfaces.

- CSCud60360

Symptoms: Active router reloads, and standby takes over.

Conditions: This symptom occurs with continuous deletion of VRFs with much less time gap between the deletions.

Workaround: Delete a few VRFs at a time with time gap between deletions.

- CSCud68830

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

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

Workaround: There is no workaround.
- CSCud71211

Symptoms: The **mpls traffic-eng reoptimize timers delay cleanup** command does not take effect in the path protection. When path protection kicks in and “mpls traffic-eng reoptimize timers delay installation” expires, the new best LSP is installed, but the protection path is torn down at the same time. This can cause a few seconds of packet drops, which are being carried over the protection LSP.

Conditions: This symptom occurs when the path protection switchover is triggered on the protected tunnel.

Workaround: There is no workaround.
- CSCud72743

Symptoms: The router crashes after issuing the **show platform nrm- mpls fid-chain handle value** command.

Conditions: If the value entered is beyond the addressable memory, the router will crash. This is an engineering command that was not intended to be viewable by customers.

Workaround: Do not issue the command except under the direction of a Cisco engineer.
- CSCud77498

Symptoms: L2 subscriber packets with new IP address on different interface would be dropped. even with the “ip subscriber l2-roaming” enabled.

Conditions: ISG should not act as DHCP server/client. Both ISG and DHCP server should be in same l2 broadcasting domain.

Workaround: Put ISG and DHCP server in different broadcasting domain.
- CSCud77762

Symptoms: The ARP packets from the subscriber are not getting resolved.

Conditions: This symptom is seen when both HSRP and **arp ignore local** are configured on an interface, and there exists a session for that mac address. The interfaces should be configured as l2-connected.

Workaround: Do not configure HSRP and **arp ignore local** on the same interface.
- CSCud78618

Symptoms: Router crashes.

Conditions: This symptom is seen when applying IVRF configuration on IKE profile.

Workaround: There is no workaround.
- CSCud83056

Symptoms: PTP session is stuck in HOLDOVER after PTP is unconfigured and configured on Master.

Conditions: This symptom occurs when unconfiguring and configuring PTP on Master.

Workaround: Do not configure below configurations as part of PTP configuration, when we do not have any physical ToD and 1PPS cables connected to Wh2.

```

tod 0/0 ntp
input 1pps 0/0

```

- CSCud90752

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

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

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

- CSCud98366

Symptoms: In a multi-home MLDP inband setup with different RDs configured, there is no MLDP state on ingress PE if BGP best path is different than multicast RPF PE.

Conditions:

1. MLDP inband profile is configured in multi-home setup with different RDs.
2. BGP chosen best path is different than chosen RPF PE for multicast.

Workaround: Configure route policy on egress PE such that chosen RPF PE is same as BGP best path.

- CSCue00690

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

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

Workaround: There is no workaround.

Open Bugs—Cisco IOS Release 15.3(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.3(1)S. All the bugs listed in this section are open in Cisco IOS Release 15.3(1)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCtj89743

Symptoms: The Cisco Catalyst 4000 series switches running Cisco IOS Release 12.2(54)SG experiences high CPU when issuing an unsupported command, **https://ip-address**, in which ip-address is accessible from this device.

Conditions: This symptom is observed with the Cisco Catalyst 4000 series switches.

Workaround: There is no workaround.

Further Problem Description: Even if SSL handshake fails, the HTTP CORE process is looping and is scheduled repeatedly.

- CSCtn70064

Symptoms: Router crashes with bus error while logging in.

Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.2(33)SRD3.

Workaround: There is no workaround.

- CSCtq56659

Symptoms: Wrong LC programming is seen with CEM interface.

Conditions: This issue is seen after the initial configuration of HSPWs.

Workaround: Soft OIR.

- CSCtr94565

Symptoms: SP is hung after the router crash.

Conditions: This symptom is seen with BGP-pic core and enabled.

Workaround: Disable the BGP pic.

- CSCtw82633

Symptoms: Flash invalid check sum is seen.

Conditions: This symptom is seen when parallel activities are going-on on flash, one from telnet and another one from vty.

Workaround: Avoid copy and write mem operations in parallel.

- CSCtx31177

Symptoms: RP crash is observed on avl search in high scaled scenario.

Conditions: This crash is seen in a high scaled scenario with continuous traffic flow.

Workaround: After removing the CLI “snmp-server enable traps resource-policy”, did not hit the crash on multiple tries.

- CSCtz50537

Symptoms: Deactivation of IPv4 unicast rpf via radius does not work.

Conditions: Occurs when you configure a user profile in RADIUS with an AVPair: Cisco-AVPair += “lcp:interface-config=no ip verify unicast source reachable-via rx”.

No error appears in debugs or logs. The same configuration works in Cisco IOS XE Release 2.x releases, but does not work in 3.x releases.

Workaround: There is no workaround.

- CSCtz63314

Symptoms: When using static multicast mac to support Microsoft NLB, multicast mac does not get programmed for the member switch. This causes the cluster to fail as the heartbeat messages will not go from the server from the member switch to the master switch.

Conditions: This happens only when one of the members in the cluster is on the member switch,

Workaround: Connect all the cluster members on the master switch.

- CSCtz91502

Symptoms: Nile unicast met shows multiple ReplicationContextQueueEntry, and traffic is flooded to all ports in VLAN.

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

Workaround: Clear mac-address table fixes the CQE entries.

- CSCua20373

Symptoms: After SSO, all the GRE tunnels get admin down and stay down until the security module SSC-600/WS-IPSEC-3 comes up. Complete traffic loss is seen during this time.

Conditions: This symptom is seen when having Vanilla GRE tunnels configured in the system where HA and IPsec Module SSC-600/WS-IPSEC-3 card is present and issue SSO.

Workaround: There is no workaround.

- CSCua23570

Symptoms: IS-IS adjacency remains down on the standby RP while it is up on the active RP. If a switchover occurs this may result in an adjacency flap as the Standby transition to Active.

Conditions: Occurs when you apply the multi-topology command under the IPv6 address family and the router receives IPv6 prefixes through IS-IS.

Workaround: There is no workaround.

- CSCua26981

Symptoms: A Cisco ASR router may crash due to a CPU Watchdog upon invocation of “show ip eigrp neighbor detail”.

```
sh ip eigrp nei detail
<snip>
ASR1000-WATCHDOG: Process = Exec
%SCHED-0-WATCHDOG: Scheduler running for a long time, more than the maximum
configured (120) secs.
-Traceback= ...
===== Start of Crashinfo Collection (09:21:44 EST Wed May 9 2012) =====
```

Conditions: This symptom occurs when the Cisco ASR router is experiencing rapid changes in EIGRP neighborhood, such as during a flap. One way to artificially create this scenario is to mismatch the interface MTU.

Workaround: There is no workaround.

- CSCua27690

Symptoms: With Xconnects (at decent scale) present in the setup, leaks are observed with clearing xconnects.

Conditions: This symptom is seen in a setup with L2VPN.

Workaround: There is no workaround.

- CSCua61201

Symptoms: Unexpected reload occurs with BFD configured.

Conditions: This symptom is seen when a device is configured with BFD. It may experience unexpected reloads.

Workaround: There is no workaround.

- CSCua64100

Symptoms: SCTP receives message fails.

Conditions: This symptom is seen when sock-test testing infrastructure is used for SCTP testing.

Workaround: Use another test tool for SCTP testing. Issue is in sock-test, not in SCTP.

- CSCua65082

Symptoms: EIGRP neighbor will not be established using GRE/NHRP.

Conditions: This symptom is seen when using GRE/NHRP.

Workaround: There is no workaround.

- CSCua75069

Symptoms: BGP sometimes fails to send an update or a withdraw to an iBGP peer (missing update).

Conditions: This problem is only seen when all of the following conditions are met:

1. BGP advertise-best-external is configured, or diverse-path is configured for at least one neighbor.
2. The router has one more BGP peer.
3. The router receives an update from a peer which changes an attribute on the backup path/repair path in a way which does not cause that path to become the best path.
4. The best path for the net in step #3 does NOT get updated.
5. At least one of the following happens:
 - A subsequent configuration change would cause the net to be advertised or withdrawn.
 - Dampening would cause the net to be withdrawn.
 - SOO policy would cause the net to be withdrawn.
 - Split Horizon or Loop Detection would cause the net to be withdrawn.
 - IPv4 AF based filtering would cause the net to be withdrawn.
 - ORF based filtering would cause the net to be withdrawn.
 - The net would be withdrawn because it is no longer in the RIB

The following releases are known to be impacted if they do not include this fix: Cisco IOS Releases 15.2T and later, 15.1S and later, 15.2M and later, 15.0EX and later. Older releases on these trains are not impacted.

Workaround: If this problem is triggered by a configuration change, subsequently do the **clear ip bgp neighbor** soft out which will resolve the situation.

- CSCua76281

Symptoms: Crash of RSP720-3C-GE @ vc_qos_change is seen.

Conditions: Device crashes unexpectedly. Last function processed was vc_qos_change.

Workaround: There is no workaround.

- CSCua95777

Symptoms: The router drops SAToP pseudowire traffic for 10 seconds following a core link failure.

Conditions: This symptom occurs when the TDM controller generates an AIS and LOF alarm following a core link failure. The router drops traffic for 10 seconds after generating the alarm.

Workaround: There is no workaround.

- CSCub04982

Symptoms: This is ipfrr configuration and the traceback is about changing the frr primary oce where the new oce has a different interface and next hop and blocks such a linkage.

Conditions: This symptom is seen while changing the frr primary oce interface to new oce with different interface.

Workaround: There is no workaround

- CSCub09099

Symptoms: When BGP MDT address-family is configured with one or more VRF having mdt default x.x.x.x with 4000 VRF out of which 400 VRF have “mdt default x.x.x.x” and with 8000 BGP neighbors in VRF (4K IPv4 & 4K IPv6), then router takes close to 30 minutes to apply the configuration.

Conditions: This will happen if neighbors configured under BGP VRF address-family with update-source command i,e **neighbor X.X.X.X update-source interface**.

Workaround: Do not use **neighbor X.X.X.X update-source interface** under BGP VRF address-family.

- CSCub11348

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

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

Workaround: There is no workaround.

- CSCub23231

Symptoms: Very specific events/packet types cause the ES20 LC to stop passing traffic. Information on these events and packets that lead to the issue are not known.

Conditions: The ES20 interface should have EVC or MPLS configuration.

Workaround: LC reload.

- CSCub23971

Symptoms: An Access-Request sent by a BRAS might miss ANCP-attributes.

Conditions: This is seen if an ANCP-enabled subinterface is set up the first time or it gets removed/re-added.

Workaround: Reconfigure the ANCP neighbor name.

- CSCub28710

Symptoms: Router crashes while running metal_te_sso_interas_cases in XE36.

Conditions: None.

Workaround: There is no workaround.

- CSCub34032

Symptoms: Traffic drop and water mark issue is seen.

Conditions: EoMPLS VC and churn the MPLS.

Workaround: There is no workaround.

- CSCub40547

Symptoms: ES+ module is crashing with “%NP_DEV-DFC1-2-WATCHDOG: Watchdog detected on NP 0”.

Conditions: None.

Workaround: There is no workaround.

- CSCub42446

Symptoms: Memory corruption is seen at cfib_rews_hwcpy.

Conditions: SP crash is observed due to memory corruption at PE3 while performing P router reload. PE3 is having l2vpn, MPLS-TE configuration.

Workaround: There is no workaround.

- CSCub68933

Symptoms: HVPLS traffic is failing to flow.

Conditions: This symptom is seen with VPLS autodiscovery in use with MPLS over SVI in the core.

Workaround: There is no workaround.

- CSCub80386

Symptoms: The following interface configuration should be used:

```
interface Ethernet2/1
description lanethernet1
ipv6 enable
ospfv3 100 network manet
ospfv3 100 ipv6 area 0
```

Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval** command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub86296

Symptoms: With OSPFv2 running between Cisco ASR 903 and Cisco 7609, if you reset OSPF on Cisco ASR 903 with “clear ip ospf process”, this can result in multiple OSPF and BFD flaps which can last up to 3 minutes sometimes.

Conditions: This symptom is seen when OSPF is the only client for BFD on Cisco 7600. Cisco ASR 903 has BFD and static routes as BFD client.

Workaround: Have a symmetric BFD client configuration.

- CSCub87579

Symptoms: MCAST traffic forwards on wrong tunnel.

Conditions: This symptom occurs only when IPsec is enabled on the interface.

Workaround: Shut and no shut of the tunnel interface resumes the traffic on the proper tunnel interface.

- CSCuc09483

Symptoms: Under certain conditions, running a TCL script on the box may cause software traceback and reload of the affected device.

Conditions: Privilege 15 user may run TCL commands that may lead to an affected device reloading.

Workaround: There is no workaround.

Further Problem Description: 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 3.8/3.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C> No CVE ID has been assigned to 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

- CSCuc10706

Symptoms: When Cisco IOS-XE is configured to use subscriber-service for authorization, it will ignore this configuration for the named list and fall back on the default for subscriber-profile or, if this is not present, on the default authorization method for the network. If none of these default authorization methods are configured, authorization will not take place.

Conditions: Named authorization list is configured.

Workaround: Set the default authorization list (subscriber-service or network) to use the correct RADIUS server.

- CSCuc11958

Symptoms: Cisco 7600-SIP-400 LC crash is seen with SPA reload.

Conditions: This issue is seen after SPA reload.

Workaround: There is no workaround.

- CSCuc13992

Symptoms: The Cisco IOSD process crashes due to a segmentation fault in the PPP process:

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events
```

The root cause for the PPP process crash is wrong IPCP option processing inside PPP control packets.

Conditions: This symptom occurs when the BRAS functionality is configured, which includes ISG and PPPoE session termination.

Workaround: There is no workaround.

- CSCuc23542

Symptoms: PXE boot is failing.

Conditions: This symptom is seen when Cisco ME 3600 running Cisco IOS Release 15.2(4)S is the DHCP relay agent.

Workaround: There is no workaround.

- CSCuc34304

Symptoms: Crash is seen in pim_reg_enc_src_update_mvrf in complex multicast setup.

Conditions: This symptom is seen when traffic is active for a combination of different IPv4 multicast vpn features/scenarios. Cisco IOS may crash upon interface coming up notification.

Workaround: There is no workaround.

- CSCuc37081

Symptoms: Incremental memory leaks observed @ EL3IDC handle, EL3IDC_VLAN shadow.

Conditions: This symptom is seen on disabling and enabling mpls traffic-eng, when the tunnel interfaces are up.

Workaround: There is no workaround.

- CSCuc48211

Symptoms: Traffic passing over the MPLS TE tunnel is dropped at the tailend. The headend is using an invalid label, unknown to the tailend.

```
TUNNEL-HEADEND#show ip cef 172.25.0.1 internal
172.25.0.0/16, epoch 6, flags rib only no-label, rib defined all labels, RIB[B],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
  IPRM: 0x00018000
  Broker: linked, distributed at 4th priority
  LFD: 172.25.0.0/16 0 local labels
      contains path extension list
  ifnums:
  TenGigabitEthernet1/0/0(31): 10.10.243.48
  Tunnel11(38)
  path 1F13EC1C, path list 1436FC80, share 1/1, type recursive, for IPv4
```

```

recursive via 10.10.254.3[IPv4:Default], fib 21B2A5CC, 1 terminal fib,
v4:Default:10.10.254.3/32
  path 13A71668, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
    MPLS short path extensions: MOI flags = 0x1 label 1683
  nexthop 10.10.243.48 TenGigabitEthernet1/0/0 label 1683, adjacency IP adj
out of TenGigabitEthernet1/0/0, addr 95.10.243.48 20BCED00
  path 13A745A8, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
    MPLS short path extensions: MOI flags = 0x1 label 623
    MPLS long path extensions: MOI flags = 0x1 label 18
  nexthop 10.10.255.130 Tunnel11 label 18, adjacency IP midchain out of
Tunnel11 22923160
  long extension for path if Tunnel11 next hop 10.10.255.130:
    MPLS long path extensions: MOI flags = 0x1 label 18
  long extension for path if Tunnel22 next hop 10.10.255.129:
    MPLS long path extensions: MOI flags = 0x1 label 651
  output chain:
    loadinfo 212F8810, per-session, 2 choices, flags 0083, 4 locks
    flags: Per-session, for-rx-IPv4, 2buckets
    2 hash buckets
    < 0 > label 1683 TAG adj out of TenGigabitEthernet1/0/0, addr
10.10.243.48 20BDC860
    < 1 > label 18 TAG midchain out of Tunnel11 20C92B00 label implicit-null
TAG adj out of TenGigabitEthernet1/0/1, addr 10.10.243.50 20B21440
  Subblocks:
    None

```

```

TUNNEL-TAILEND# sh mpls forwarding-table labels 18
Local      Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label      Label     or Tunnel Id    Switched     interface
TUNNEL-TAILEND#

```

Conditions: This symptom occurs when the prefix is learned by both BGP and IGP, while BGP has lower Administrative Distance, pointing via the MPLS TE tunnel carrying MPLS. This issue is seen once the prefix is installed to RIB by IGP and then by BGP (Reload, BGP flap, etc.); then, the CEF will keep using the IGP/LDPs label without updating it in case of LDP label change.

Workaround: Issue the **clear ip route prefix mask** command.

- CSCuc49335

Symptoms: An infinite loop is seen at tunnelInetConfigIfIndex.ipv6 while doing SNMP walk.

Conditions: This symptom occurs when an SNMP walk is done on the Cisco ISRG2 router and the Cisco ASR 1000 router.

Workaround: There is no workaround.

- CSCuc49814

Symptoms: Unable to start capture with inline ipv6 filter.

Workaround: Create ipv6 ACL through config mode and attach it to capture fix: fixed PI code to successfully create ACL for capture.

- CSCuc50162

Symptoms: Cisco IOSD crashes on the setup having scaled VPLS and CFM configuration.

Conditions: The setup has VPLS instances around 3500 and CFM meps around 1600. The issue is not consistently reproducible.

Workaround: There is no workaround.

- CSCuc54815

Symptoms: VLAN-based EoMPLS pseudowire over TE tunnel is not working.

Conditions: This symptom is seen when mac learning is enabled for that VLAN.

Workaround: Disable mac learning for that VLAN.

- CSCuc55634

Symptoms: IPv6 static route cannot resolve the destination.

Conditions:

1. We have a VRF configured by the old style CLI (For example “ip vrf RED”).
2. Configure “ip vrf forwarding RED” under an interface
3. Configure IPV6 address under the same interface (For example 2001:192:44:1::2/64)
4. Configure IPV6 static route via the interface configured in 3). (For example IPv6 route 2001:192:14:1::/64 2001:192:44:1::1).
5. Then, we are not able to ping the “2001:192:14:1::2” although we can reach to “2001:192:44:1::1”.

Workaround: There is no workaround.

- CSCuc57360

Symptoms: Adjacencies in the stats region gets exhausted.

Conditions: This symptom is seen when reloading the router with mldp inband v4 and v6 data and control traffic being on, with other features configured (scaled config), the adjacency leak happens. Adjacency allocation failure happens for the adjacencies allocated during this time.

Workaround: There is no workaround.

- CSCuc57499

Symptoms: With IPv6 BGP C-Multicast routes, executing “clear ip ospf process” results in a long convergence time for IPv6 multicast traffic

Conditions: This issue is seen when BGP dampening is configured for IPv6 BGP MVPN. After “clear ip ospf process”, IPv6 multicast routes in the VRF flap once too often (due to RPF changes resulting for VPNv6 route withdrawal and IPv6 PIM neighbor expiry). These flaps lead BGP to dampen the advertisement of IPv6 BGP C-Multicast routes and hence the long time for traffic to recover.

Workaround: Configure more flexible BGP dampening parameters for IPv6 MVPN (under **address-family ipv6 mvpn vrf name** BGP sub-mode). One such example of BGP dampening parameters is **bgp dampening 5 3000 4000 10**. Another workaround is to disable BGP dampening for IPv6 MVPN.

- CSCuc58922

Symptoms: The process “AAA aux” leaks memory at radius_sg_pm_coa_server and aaa_req_alloc on Cisco ASR 1000.

```
BRN020-RASR1006-1# show process memory 166
Process ID: 166
Process Name: AAA aux
Total Memory Held: 716372648 bytes
```

```
Processor memory Holding = 716374560 bytes
pc = 0x023BB7A6, size = 383262816, count = 438321
pc = 0x00A89E6A, size = 255990888, count = 438321
pc = 0x00A89E3D, size = 76959728, count = 438322
pc = 0x00ABAD2F, size = 131264, count = 2
pc = 0x03CB1434, size = 28192, count = 1
pc = 0x0280BB67, size = 1224, count = 1
pc = 0x02805898, size = 448, count = 1
```

PC decode:

0x023BB7A6: __be_radius_sg_pm_coa_server(0x23bb5b0)+0x1f6

0x00A89E6A: __be_aaa_req_alloc(0xa89da0)+0xca

0x00A89E3D: __be_aaa_req_alloc(0xa89da0)+0x9d

0x00ABAD2F: __be_make_a_sublist_max(0xabad00)+0x2f

0x03CB1434: __be_mcp_vm_malloc_bounded_fn(0x3cb13e0)+0x54

0x0280BB67: __be_process_create_common(0x280ba90)+0xd7

0x02805898: __be_process_malloc_event_set(0x2805860)+0x38

Conditions: This symptom is seen when a lot of COA requests are coming from a RADIUS server at the same time.

Workaround: There is no workaround.

- CSCuc59049

Symptoms: Cisco ME 3800X crashinfo files may be corrupted.

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

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

- CSCuc59105

Symptoms: Switch may crash when running “show platform qos policer cpu x x”.

Conditions: The crash is only seen when running through an SSH session and with AAA configured.

Workaround: Run the commands through telnet or console.

- CSCuc59765

Symptoms: Cisco ME 380X/ME 360X fails to trigger watchdog crash in certain scenarios.

Conditions: Soaking over a prolonged period of time.

Workaround: This is no workaround.

- CSCuc60245

Symptoms: Pseudowires stop passing traffic until lsp reopt.

Conditions: None.

Workaround: Reoptimize the LSP onto a new path in one or both directions.

- CSCuc65096

Symptoms: MVPNv4/MVPNv6 Traffic is not flowing properly after removing/adding MDT configs.

Conditions: When default mdt <multicast-group> is removed/added from/to VRF IPv4/IPv6 address-family then MVPNv4/MVPNv6 traffic is not converged.

Workaround: Issue “clear ip bgp vpnv4/vpnv6 unicast <asnum> soft out” whenever mdt is configurations is removed or added back.

- CSCuc65424

Symptoms: A route processor might crash without a visible trigger.

Conditions: No specific condition is identified contributing to the crash.

Workaround: There is no workaround.

- CSCuc72244

Symptoms: On the Cisco 7609, both sides running Cisco IOS Release SRE4 SIP-400 with SPA-2X1GE-V2 configured with “negotiation Auto” and changed to “no negotiation auto”. The GE interface of the router is operating in half-duplex mode after falling back. The interface is operating in half-duplex instead of the expected (nonconfigurable) full-duplex.

Conditions: This symptom does not occur under any specific conditions. This issue is observed due to a timing constraint upon updating the duplex state.

The steps to reproduce are as follows:

1. The interface in Router A is configured to “negotiation auto” with no change in duplex state on both sides.
2. The interface in Router B is configured to “negotiation auto” with no change in duplex state on both sides.
3. The interface in Router A is configured to “no negotiation auto”. The duplex state for both interfaces is changed to half-duplex.
4. The interface in Router B is configured to “no negotiation auto”. The interface duplex state for Router B is changed to full-duplex. But, the Router A interface remains in half-duplex.

Workaround: There is no workaround.

- CSCuc73473

Symptoms: IPv6 default route is not redistributed in BGP (VRF).

Conditions: OSPFv3 with “default-information originate always” is configured in the same VRF.

Workaround: To clear the issue: cle ip bg * to avoid the issue: remove “default-information originate always” from OSPFv3 in respective VRF.

- CSCuc76515

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

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

Workaround: Clear xconnect peer.

- CSCuc77283

Symptoms: Upon reload or OIR, CFM MEP configuration on an xconnect EFP is removed and cannot be re-configured.

Conditions: This symptom is seen with CFM MEP on xconnect service instance. Reload or OIR is performed.

Workaround: Remove domain configuration.

- CSCuc78051

Symptoms: With the command **radius source port extended** the router should increase the UDP source port whenever the Radius ID wraps around. In circumstances where there is a burst of Requests when the Radius ID wraps around, the router may not increase the UDP source port.

Conditions: This symptom is seen when “radius source port extended” is configured, and there is a burst of RADIUS requests when the Radius ID wraps around.

Workaround: There is no workaround.

- CSCuc78772

Symptoms: CPU watchdog is observed, followed by the box crashing.

Conditions: This symptom occurs when an IPv6 ACL entry is created with the log option. If there are more than 16 different traffic matching this ACL with a high rate, the box will run out of CPU to send to the log.

Workaround: Remove the log option from the ACL entry or create a more specific ACL to get less than 16 different traffic matching the same ACL entry.

- CSCuc79161
Symptoms: Memory leak is seen.
Conditions: This symptom occurs after flapping the interface and keeping the setup idle and executing CLI clear xconnect all results in memory leaks.
Workaround: There is no workaround.
Further Problem Description: The PI front-end pseudoport is not deleted when the xconnect is removed which causes the memory leak. It is because PD returns BDOMAIN_PP_FAILED to PI when pp_engine_context is a NULL pointer.
- CSCuc79923
Symptoms: On a Cisco 7600 running Cisco IOS Release 15.2(4)S1, packets from FWSM are dropped when the servicemodule session is enabled. Ping fails for the VLAN interface on the FWSM module from the supervisor. The ARP entry is incomplete on the Cisco 7600.
Conditions: This symptom is observed with the following conditions:
 - This issue is seen on the Cisco 7600 with FWSM and SUP-720-3B running Cisco IOS Release 15.2(4)S1.
 - The FWSM is in Crossbar mode.
 - The system is in “distributed” egress SPAN replication mode.This issue is not seen with Cisco IOS Release 12.2(33)SRE7.
Workaround:
 - Disable the servicemodule session.
 - Change the fabric switching mode to bus.
 - Change SPAN egress replication mode to “centralized”.
- CSCuc82551
Symptoms: Cisco ASR 1001 that is running Cisco IOS Release XE 3.6.2 or 3.7.1 crashes with SNMP traffic.
Conditions: SNMP polling with IP SLA configurations should be configured.
Crash signature: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
Workaround: Remove SNMP configuration from the router or schedule the probe before polling via SNMP.
- CSCuc85297
Symptoms: If a Cisco 7600 router’s Cisco IOS image is upgraded using the ISSU procedure, the P2P tunnel interface multicast traffic might be affected.
Conditions: This occurs with a Cisco IOS Release 12.2SRE7-based release.
Workaround: Perform a **shut/no shut** of the P2P tunnel interface.
- CSCuc85609
Symptoms: Packet drops (%0.0016) on Cisco 7600 over mGRE tunnels (dmvpn setup).
Conditions: This symptom is observed with Cisco IOS Release 15.1(3)S while ingress/egress LC is WS-X6748-GE-TX. No issue is seen when traffic is routed over p2p GRE tunnel.
Workaround: There is no workaround.
- CSCuc90580
Symptoms: Ping fails over RoutedPW.

Conditions: This symptom is seen with SVI based MPLS uplink.

Workaround: Disable MAC learning.

- CSCuc92345

Symptoms: When establishing dualstack PPPoE session on Cisco ASR 1000 router, IPv6 CP is not open when RADIUS user profile contains VRF attribute (session should be put in VRF), and “lcp:interface-config=ipv6 enable” attribute is not used.

Conditions: This issue is seen on a Cisco ASR 1000 router, on Cisco IOS Releases 15.1(3)S0a and 15.2(4)S1.

Workaround: When “lcp:interface-config=ipv6 enable” IPv6 CP is opened correctly.

- CSCuc94983

Symptoms: Node crashes.

Conditions: This issue is seen with rigorous flapping of the core.

Workaround: Have a stable core network.

- CSCuc95398

Symptoms: Imposition L3VPN traffic fails.

Conditions: This issue is seen with traffic moving from TE tunnel to ECMP paths.

Workaround: Get the TE tunnel working.

- CSCuc95987

Symptoms: Memory related crash seen with RLS13 image in high scale scenario. Here RP is being reset by SP. But SP crashinfo always shows as size zero in sup-bootflash. Issue is seen while power disable/enable module (LC) test.

Conditions: The symptom is observed with the following router configurations:

L2VPN: scale number

- 8.5 EVC = 2.5K EVC+BD + 6K EVC.
- 9k VCs (2.5kvpls + 6kscalable + 500 software EoMPLS).
- 5 primary tunnel and 5 backup tunnel towards core.

L3VPN: scale number

- 50 vpn and 100 flows per vpn - interfaces mix with MLPP, Gig.

ACL:

- 1K I3/I4 ACL.

Workaround: There is no workaround.

- CSCuc96345

Symptoms: ARP exchange between Cisco 7600 and client device fails. Cisco 7600 has incomplete ARP entry in its ARP table for client. This is likely to be seen between Cisco 7600 and other Cisco platforms with MAC address 6073.5Cxx.xxxx. Incoming ARP reply is parsed by platform CEF as IP packet and dropped.

The following OUIs (as of 30 Oct 2012) are affected:

(first 3 bytes from MAC address/MAC starts with)

14-73-73
20-73-55
4C-73-67

4C-73-A5
 54-73-98
 60-73-5C (One of Cisco's OUI Ranges)
 64-73-E2
 70-73-CB
 8C-73-6E
 98-73-C4
 A0-73-32
 C4-73-1E
 D0-73-8E
 F0-73-AE
 F4-73-CA

Conditions: EVC pseudowire and 802.1q subinterface on same physical interface, connectivity via subinterface affected.

Sample configuration:

```
interface TenGigabitEthernet3/1
  service instance 2013 ethernet
    encapsulation dot1q 411 second-dot1q 200
    rewrite ingress tag pop 2 symmetric
    xconnect 10.254.10.10 3350075 encapsulation mpls
interface TenGigabitEthernet3/1.906
  encapsulation dot1Q 906
  ip address 10.10.10.1 255.255.255.0
```

Workaround:

- Static ARP entry on 7600 for client's MAC & IP
- Change MAC address of client to non-affected OUI.

- CSCuc97995

Symptoms: PPPoE subscriber stops coming online.

Workaround:

1. Remove radius attribute "ip mtu x" from user profile.
2. Remove accounting list from the service applied to subscriber.

- CSCuc98226

Symptoms: When a PC is moved between two VLAN ports several times by its LAN cable connection on the L2SW which is connected to the Cisco ASR 1000 router, the PC becomes unable to acquire an IP address from DHCP on the Cisco ASR 1000 router. At that time, an incorrect interface is shown in show ip dhcp binding.

Conditions: The symptom is observed with Cisco IOS Release 15.2(4)S1.

Workaround: There is no workaround.

- CSCud03273

Symptoms: All the paths using certain nexthops under the route-map are marked inaccessible.

Conditions:

1. Configure peer groups.
2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).
3. Configure Prefix-list.
4. Configure route-map.
5. Configure BGP neighbor and add them to peer-groups.

Workaround: Configure “route-map permit <seq-num> <name>” or activate at least one neighbor in “address-family ipv4”.

- CSCud06438

Symptoms: IP Sessions do not come up after the DHCP failure is encountered.

Conditions: This symptom occurs when the DHCP address pool is not configured in the DHCP server and if a DHCPDISCOVER request is sent from the client to the server.

Workaround: There is no workaround.

- CSCud08166

Symptoms: Cisco ASR 1000 router crashes with “Exception to IOS Thread” and “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Virtual Exec”.

Conditions: An ACL used with “ip pim rp-address” is moved from standard to extended and “no ip multicast-routing” is configured (either in global or in a mvrf). The standard ACL must be deleted and recreated as extended. e.g. The following series of commands are necessary to trigger the crash:

```
<begin-config>
!
ip multicast-routing
!
ip pim rp-address 10.200.255.42 STATIC-RP-LN-SERVER-FARMS override
!
no ip access-list standard STATIC-RP-LN-SERVER-FARMS
ip access-list extended STATIC-RP-LN-SERVER-FARMS
 remark -- STATIC RP LN SERVER FARMS MCAST GROUP ACL --
 permit ip 239.255.0.0 0.0.255.255 any
 permit ip 224.0.0.0 15.255.255.255 any
!
!
no ip multicast-routing
<end-config>
```

Workaround: Crash can be prevented by any of the following methods:

1. Disassociate the standard ACL from “ip pim rp-address” before deleting ACL. e.g. “no ip pim rp-address 10.200.255.42 STATIC-RP-LN-SERVER-FARMS override” and then “no ip access-list standard STATIC-RP-LN-SERVER-FARMS”.
 2. Do not convert a standard ACL to extended while it is still being referenced in “ip pim rp-address”. Use a new name for the new extended ACL.
 3. Do not disable multicast routing using “no ip multicast-routing”.
- CSCud09627

Symptoms: Error messages “npm_intfman_get_el3idc_vlan_index:interface el3id handle is NULL” are seen on the console

Conditions: This symptom occurs with the following:

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

or on doing IM OIR on peer end

Workaround: There is no workaround.

- CSCud11627

Symptoms: SUP720 supervisor module may hang in ROMMON after the module reset that is triggered by TM_DATA_PARITY_ERROR.

Conditions: This issue is observed after the module reset that is triggered by TM_DATA_PARITY_ERROR.

Workaround: Power off/power on the router.

- CSCud13862

Symptoms: The Cisco WS-SUP720 running Cisco IOS Release 12.2(33)SRE3 crashes.

Conditions: This symptom occurs during a CPU process history update.

Workaround: There is no workaround.

- CSCud14605

Symptoms: Trace back is seen @ %PLATFORM_NCEF-3-LB: Linktype 90 not supported:LB update while testing bgp_3ias script.

Conditions: None.

Workaround: There is no workaround.

- CSCud16693

Symptoms: Cisco ME 3600X/ME 3800X switch crashes as soon as policy-map referencing table-map is applied.

Conditions: This symptom occurs when applying service policy, which has unsupported combination of police action with table-map and without table-map.

Workaround: Configure service policy, which does not have the combination of police action with table-map and without table-map.

- CSCud17934

Symptoms: PW redundancy on Cisco 7600 does not work when primary VC goes down and backup VC takes over, and CE to CE communication gets broken.

Conditions: This symptom occurs when MPLS facing LC is WS-X6704-10GE CE facing LC is ES+.

Workaround: Use other HW on MPLS core.

- CSCud19257

Symptoms: NAT CLIs expose “vrf” keyword on Cisco 7600, which is not supported.

Conditions: This issue is seen with NAT configuration.

Workaround: Do not use “vrf” in NATing on Cisco 7600.

- CSCud20092

Symptoms: The switch crashes.

Conditions: This symptom occurs when you apply policy-map referencing table-map to a service instance on a switch port.

Workaround: There is no workaround. The CLI is unsupported.

- CSCud22222

Symptoms: Router crashes upon ISIS neighbor up event when ISIS fast-reroute is enabled.

Workaround: Remove isis fast-reroute from configuration.

- CSCud22437

Symptoms: A Cisco ASR 1000 router may experience a watchdog crash due to a kernel panic. Upon viewing the plaintext contents of the resultant kernel core file that is generated, IOSD generates a watchdog because of a soft lockup that prevents it from responding within 60 seconds:

<3>BUG: soft lockup - CPU#0 stuck for 61s! [linux_iosd-imag:26869]
 Conditions: No particular conditions are required.

Workaround: There is no workaround.

- CSCud24364

Symptoms: WS-X6704-10GE card does not boot up post reload in RLS13 images with the below log:

```
%OIR-SP-3-UNKNOWN: Unknown card in slot 9, card is being disabled
```

Workaround: Issue “hw-module mod <> reset”.

- CSCud24977

Symptoms: Crashes are observed on ISG ASR device with no trigger for the crashes.

Conditions: This symptom is seen in ES special image ES Image:

```
asr1000rp2-adventerprisek9.V152_1_S1_CSCTY21366_2.bin  

  in Cisco IOS Release 15.2(1)S2.
```

Workaround: There is no workaround.

- CSCud25168

Symptoms: The crash traceback decode seems to refer towards DHCPD process, but the immediate functions reside in AAA.

Conditions: The crash is seen in AAA function and may be related to CSCud24977.

Workaround: There is no workaround.

Further Problem Description: Right before the crash, there were a few bad aaa handle (%AAA-6-BADHDL: invalid hdl AAA ID) errors in a row.

- CSCud26339

Symptoms: Changing policy-map parameters triggers an IOSD crash.

Conditions: This issue is seen when policy map is attached to a service instance on Cisco ASR 903.

Workaround: Remove the policy-map from the target and then make the changes.

- CSCud27379

Symptoms: WS-SUP720-3B that is running Cisco IOS Release 12.2(33)SRE4 crashes at get_alt_mod after issuing “sh run int g4/13” with several trailing white spaces until cursor stops moving.

Conditions: This symptom is seen when issuing the **show run interface** command with trailing spaces until cursor stops moving.

Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud28177

Symptoms: Updates are not advertised after IPv4 BGP session is restored.

Conditions: This issue is seen when BGP is restored. Routes are not advertised to neighbor.

Workaround: Hard reset BGP session to the affected neighbor or shut down link or BGP from where the updates originate.

Resolved Bugs—Cisco IOS Release 15.3(1)S

All the bugs listed in this section are resolved in Cisco IOS Release 15.3(1)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCej11786

Symptoms: A Cisco router reloads when the **clear counter** command is performed on the router. This crash is reproducible only after making a number of calls first.

Conditions: This symptom has been observed on Cisco 2600, Cisco 3845, and Cisco 7200 routers.

Workaround: There is no workaround. The crash can be avoided by not issuing the **clear counter** command.

- CSCsl38246

Symptoms: When console logging is turned on, a flood of the messages shown below:

```
%MWAM-DFC3-0-CORRECTABLE_ECC_ERR: A correctable ECC error has occurred,  
A_BUS_L2_ERRORS: 0x0, A_BUS_MEMIO_ERRORS: 0xFF, A_SCD_BUS_ERR_STATUS: 0x80DC0000  
can potentially lead to watchdog invocation and a subsequent crash.
```

Conditions: A single-bit correctable error is detected on a CPU read from DRAM. As long as the errors remain correctable, and the performance of the processor does not deteriorate, the module is usable.

Workaround: Since this is a parity error you can prevent the issue from happening in the future by reseating the module. If the issue still persists after reseating the module then we may be facing a hardware issue.

- CSCso75347

Symptoms: When “cable dhcp-giaddr policy strict” is configured at the Cisco CMTS, the CPEs behind the CMs are expected to get the DHCPOFFER message with its source IP address belonging to secondary IP Network Address range of the downstream cable interface in the CMTS.

Currently the DHCPOFFER has the source IP-Address from the downstream primary IP Network address range.

Conditions: The issue occurs when “cable dhcp-giaddr policy strict” CLI is configured at the CMTS cable downstream interface.

Workaround: There is no workaround.

- CSCsq83006

Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.

Workaround: Use the port-channel interface settings below:

```
(config)# interface port-channel <port-channel interface number>  
(config-if)# bandwidth <bandwidth value>  
(config-if)# delay <delay value>
```

Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- CSCsr06399

Symptoms: A Cisco 5400XM may reload unexpectedly.

Conditions: This symptom is intermittent and is seen only when the DSPs available are insufficient to support the number of calls.

Workaround: Ensure that sufficient DSPs are available for transcoding.

- CSCtd43540

Symptoms: Memory leak at `cdp_handle_version_info`. This problem was triggered by misbehavior of peer switch running Cisco IOS Release 12.2(46)SE.

Conditions: The symptom is observed with link flapping.

Workaround: Disable CDP on the flapping interface.

- CSCtd54694

Symptoms: A crash is seen for the **show cdp neighbor port-channel no** and **show cdp neighbor port-channel no de?** commands.

Conditions: This symptom is a rare timing issue.

Workaround: Use the **show cdp neighbor** and **show cdp neighbor detail** commands for brief and detailed CDP information. Also, the **show cdp neighbor interface type no** can be used with the exception that the *interface type* argument should not be *port-channel*.

- CSCtd58886

Symptoms: The CMTs crash when SNMP client is inquiring `ifRcvAddressEntry`, which has a non-zero address of a GE interface in SPA.

Conditions: This symptom is observed on a Cisco uBR10000 with 5GE SPA that is running Cisco IOS Release 12.2SCB or 12.2SCC with the following:

```
SNMP command: "getnext -v2c x.x.x.x(cmts address) [community]
ifRcvAddressStatus(or ifRcvAddressType).11(ifIndex of GE in
SPA).6.2.0.0.0.0.160(an non-zero address)"
```

Workaround: Do not query this entry of the table, since it does not exist.

- CSCtg39957

The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate this vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp>

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

- 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

- CSCtg73812

Symptoms: A device running Cisco IOS may reload unexpectedly.

Conditions: This symptom is observed with a device that has HSRP and IP SLB configuration. This appears to happen during a period of HSRP flapping.

Workaround: There is no workaround.

Further Problem Description: It is believed that the crash is seen if a SLB probe is sent out of the active interface, but received after an HSRP switchover when it is no longer active. Addressing the cause of the HSRP flaps would prevent this from happening.

- CSCth71093

Symptoms: Routers configured to dump core to flash: or flash0: fail to dump correctly to 4GB CompactFlash card.

Conditions: The symptom is observed with the following configuration:

(Cisco 3925) exception flash all flash0:

(Cisco 3825) exception flash all flash:

Then when you issue a **wr core**, it fails to dump core files.

Workaround: Dump cores to TFTP.

- CSCti53665

Symptoms: Memory leak occurs from the line card in small SNMP chunks.

Conditions: This issue occurs when data and PCMM voice traffic runs continuously on the Cisco uBR-MC3GX60V line card.

Workaround: Do not enable SNMP pooling on the system.

- CSCti62247

Symptoms: If an IPv4 or IPv6 packet is sent to a null interface, a Cisco ASR 1000 series router will not respond with an ICMP or ICMPv6 packet.

Conditions: This symptom occurs with a prefix routed to Null0 interface.

Workaround: There is no workaround.

- CSCtj93356

Symptoms: Batch suspending from platform causes the MFIB on line card to go into reloading state.

Conditions: This symptom occurs when MFIB on line card goes into reloading state and then finally to purge state after removal/addition of MVRFs is done followed by a line card reset.

Workaround: There is no workaround.

- CSCtk15666

Symptoms: Cisco IOS password length is limited to 25 characters.

Conditions: This symptom is seen on NG3K products.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

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

- CSCtl86057

Symptoms: The loading of the standby RP and bulk sync times has increased on the XE3 throttle. Increases in time of up to 20-30% have been seen.

Conditions: This problem becomes more noticeable under higher scale.

Workaround: There is no workaround.

- CSCtl87463

Symptoms: Queue length becomes negative.

Conditions: The symptom is observed when Cisco IOS-WAAS is configured on the interface.

Workaround: There is no workaround.

- CSCto59459

Symptoms: Connections that are optimized by WAAS are reset. Malformed TCP options are added to the packet that is created and sent by WAAS-Express over the WAN, causing the peer WAE to reset connections.

Conditions: Any TCP connection will suffer from this defect.

Workaround: There is no workaround.

- CSCto87436

Symptoms: In certain conditions, a Cisco IOS device can crash, with the following error message printed on the console:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc
```

Conditions: In certain conditions, if an SSH connection to the Cisco IOS device is slow or idle, it may cause a box to crash with the error message printed on the console.

Workaround: There is no workaround.

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 6.3/5.5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C> CVE ID CVE-2012-5014 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

- CSCtq17444

Symptoms: A Cisco AS5400 crashes when performing a trunk call.

Conditions: The following conditions are observed:

- Affected Cisco IOS Release: 15.1(3)T.
- Affected platforms: routers acting as voice gateway for H.323.

Workaround: There is no workaround.

- CSCtq24011

Symptoms: Routers act as though local-proxy-arp is configured and will do a proxy-arp even for the systems in the same subnet.

Conditions: The router receives ARP request on an interface while the interface is not fully initialized. The connected routes are not added in the routing table yet. This causes proxy-arp reply and wrong ARP entry is stuck.

Workaround: Shut/no shut on victim and offender routers.

- CSCtq41512

Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to Multi-frame established.

Conditions: This symptom occurs when “voice-class busyout” is configured and the controller TEI comes up before the monitored interface.

Workaround: Remove the “voice-class busyout” configuration from the voice-port.

- CSCtq97883

Symptoms: Traceback is shown. The root cause is a null pointer.

Conditions: The symptom is observed during longevity testing of Cisco IOS Release 12.4(24)GC3a and Release 15.1(2)GC.

Workaround: There is no workaround.

- CSCtr10577

Symptoms: The following error message may be seen:

```
OCE-3-OCE_FWD_STATE_HANDLE limit reached.
```

Conditions: This symptom is observed under high traffic.

Workaround: There is no workaround.

- CSCtr45030

Symptom: The SNMP timers process causes the router to exit global configuration mode or prevents the console from entering global configuration mode.

```
c7609#conf t
```

```
Configuration mode is locked by process '319' user 'unknown' from terminal '0'. Please try later.
```

```
c7609#show proc | in 319
```

```
319 Mwe 9735348          928      21701      42 4412/6000    0 SNMP Timers
```

Or

```
c7609(config)#logging console
```

```
Config session is locked by process '307', user will be pushed back to
exec mode. Command
execution is locked, Please try later.
```

```
c7609 (config)#^Z
```

Conditions: Occurs when you copy and paste large configurations, particularly a large number of VLAN configurations. The issue occurs without any SNMP configurations present.

Workaround:

- Option 1: Disable RMON.
 - Option 2: If configuration is huge, paste in multiple blocks.
 - Option 3: Enable debug snmp timers. Paste the required configuration when the timer callbacks have finished executing.
- CSCtr45287

Symptoms: Router crashes in a scale DVTI scenario.

Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.

Workaround: Use fewer tunnels or use a different platform.

- CSCtr45978

Symptoms: Cisco IOS WAAS has FTP or HTTP connections hung in CONN_ABORT state.

Conditions: This symptom is seen when device is configured with Cisco IOS WAAS. Crafted FTP packets or real HTTP user traffic to internet sites is passed across the WAN link. Has only been observed on Cisco IOS Release 15.2(1)T.

Once the connection limit is reached, the rest of the connections start going pass-through.

Workaround: There is no workaround.

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 5/4.1:

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

No CVE ID has been assigned to 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

- CSCtr87413

Symptoms: Static route that is injected by “reverse-route static” in crypto map disappears when the router receives the delete notify from the remote peer. Static route also gets deleted when DPD failure occurs.

Conditions: The symptom is observed when you configure “reverse-route static” and then receive a delete notify or DPD failure.

Workaround: Use **clear crypto sa**.

- CSCtr93412

Symptoms: Crash seen on mwheel process.

Conditions: The symptom is observed with GETVPN multicast followed by **clear crypto gdo**.

Workaround: There is no workaround.

- CSCts00341

Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server server.domain.com**, the command fails with the following message on the console:

```
ASR1k(config)#ntp server server.domain.com          <<<   DNS is not resolved
with dual RPs on ASR1k
Translating "server.domain.com "...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn't support this command          ^
% Invalid input detected at '^' marker.
```

```
ASR1k(config)#do sh run | i ntp
ASR1k(config)#
```

Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts01653

Symptoms: Spurious memory access seen on video monitoring router.

Conditions: The issue is seen after recreating the interface.

Workaround: There is no workaround.

- CSCts08224

Symptoms: Expected ACL/sessions not found for most of the protocols.

Conditions: The symptom is observed with expected ACL/sessions.

Workaround: There is no workaround.

- CSCts12499

Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

Workaround: There is no workaround.

- CSCts44393

Symptoms: A Cisco ASR 1000 crashes.

Conditions: The symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

Workaround: There is no workaround.

- CSCts47776

Symptoms: Router crashes due to Mediatrace performance monitor debug.

Conditions: The issue is seen with debug performance monitor database.

Workaround: There is no workaround.

- CSCts54641

Symptoms: Various small, medium, or big VB chunk leaks are seen when polling EIGRP MIB or during SSO.

Conditions: This symptom is observed when MIBs are being polled or SSO is done.

Workaround: There is no workaround.

- CSCts55778

Symptoms: This is a problem involving two SAF forwarders, where one is running EIGRP rel8/Service-Routing rel1 and the other is running EIGRP dev9/Service-Routing dev2. The capabilities-manager, a client of the service-routing infrastructure, will advertise 2 services. When forwarders are peering with the same release image, the services propagate between the forwarders without any problems. But, when you run rel8/rel1 on one forwarder, and dev9/dev2 on the other forwarder, a third service appears in the topology table and the SR database that was not advertised. Note: The problem cannot be recreated if both forwarders are running an Cisco IOS XE Release 3.4S or Cisco IOS XE Release 3.5S image.

Conditions: This symptom occurs if two SAF forwarders peer with each other, where one SAF forwarder is running EIGRP SAF rel9 or above and the other SAF forwarder is running EIGRP SAF rel8 or below.

Workaround: Make sure each SAF forwarder is running EIGRP rel8 or below, or rel9 or above.

- CSCts68626

Symptoms: PPPoE discovery packets causes packet drop.

Conditions: The symptom is observed when you bring up a PPPoE session and then clear the session.

Workaround: There is no workaround.

- CSCts89761

Symptoms:

1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

```
Router(config)#interface GigabitEthernet0/2/1
Router(config-if)#service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)#match access-group 110
Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this point,
all configs will print out an error message
Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted
Router(config-spolicy-inline-mparam)#interval duration 10 <----- Not accepted
Router(config-spolicy-inline-mparam)#history 5 <----- Not accepted
```

2. Non-inline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

```
UUT_451(config)#policy-map type performance-monitor VM_POLICY
UUT_451(config-pmap)#class VM_CLASS
UUT_451(config-pmap-c)#flow monitor VM_MONITOR
UUT_451(config-pmap-c)#monitor parameters
UUT_451(config-pmap-c-mparam)#history 6 <----- Error message will show
up if previous history value is different
UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will
show up if previous interval duration is different
UUT_451(config-pmap-c-mparam)#react 102 mrv <----- Error message will show
up if this react was not configured before or if the subsequent command
changes the threshold value of the already-configured react.
```

Conditions:

1. This symptom is seen when configuring an inline service policy for performance monitor on ASR platform.

2. This symptom is seen when modifying monitor parameters of a non-inline service policy for performance monitor on a Cisco ASR platform.

Workaround:

1. To configure inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also the changes do not apply if you specify an “empty” flow monitor, for example a flow monitor without an enclosing valid flow record.

- CSCtt15963

Symptoms:

1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

```
Router(config)#interface GigabitEthernet0/2/1
Router(config-if)#service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)#match access-group 110
Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this point, all
configs will print out an error message Router(config-if-spolicy-inline)#monitor
parameters <----- Not accepted Router(config-spolicy-inline-mparam)#interval duration
10 <----- Not accepted Router(config-spolicy-inline-mparam)#history 5 <-----
Not accepted
```

2. Non-inline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

```
UUT_451(config)#policy-map type performance-monitor VM_POLICY
UUT_451(config-pmap)#class VM_CLASS
UUT_451(config-pmap-c)#flow monitor VM_MONITOR UUT_451(config-pmap-c)#monitor
parameters UUT_451(config-pmap-c-mparam)#history 6 <----- Error message will
show up if previous history value is different
UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will show up if
previous interval duration is different
UUT_451(config-pmap-c-mparam)#react 102 mrv <----- Error message will show up if
this react was not configured before or if the subsequent command changes the
threshold value of the already-configured react.
```

Conditions:

1. This symptom is seen when configuring an inline service policy for performance monitor on ASR platform.
2. This symptom is seen when modifying monitor parameters of a non-inline service policy for performance monitor on a Cisco ASR platform.

Workaround:

1. To configure inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also the changes do not apply if you specify an “empty” flow monitor, for example a flow monitor without an enclosing valid flow record.

- CSCtt21228
Symptoms: Router crashes while trying to configure Tcl script via SSH connection.
Conditions: SSH to the router and then try to configure Tcl script.
Workaround: There is no workaround.
- CSCtt45381
Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace>
- CSCtt70133
Symptoms: The RP resets with FlexVPN configuration.
Conditions: This symptom is observed when using the **clear crypto session** command on the console.
Workaround: There is no workaround.
- CSCtu07968
Symptoms: A Cisco 890 router may provide incorrect performance monitor statistics and omit some incoming packets from being handled by flexible netflow.
Conditions: This is observed when performance monitoring or flexible netflow is enabled with IPsec over a tunnel on an input interface.
Workaround: There is no workaround.
- CSCtu16862
Symptoms: L4F tracebacks observed with SMB stress test traffic. You may experience a couple of retransmissions due to that and some small performance degradation.
Conditions: The symptom is observed with stress testing.
Workaround: There is no workaround.
- CSCtu23195
Symptoms: SNMP ifIndex for serial interfaces (PA -4T/8T) becomes inactive after PA OIR.
Conditions: The symptom is observed with a PA OIR.
Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.
- CSCtu29815
Symptoms: If the CCM sub is restarted before the switchover from PUB to SUB, the MGCP GW needs at least 10 minutes to finish the switchover.

Conditions: The symptom is observed under the following conditions:

- MGCP GWx1.
- Version: c2800nm-spsservicesk9-mz.151-3.T.bin.
- CUCM: version 8.6.1x2.
- Primary CCMPUB and CCMSUB.

Workaround: Restart the MGCP process from the gateway by using **no mgcp** and **mgcp**.

Further Problem Description: When the CCMSUB's service is down (or machine is powered off), CM service sends a TCP FIN to MGCPGW, however from the debug of MGCPGW, the backhaul link between CCMSUB does not refresh as the TCP layer is stuck at CLOSEWAIT. It is confirmed that the MGCP GW is not notified about this at all, or the MGCP GW does not actively check the status the backup backhaul link.

Then CCMSUB's started/powerd on/recovered, however the CCMPUB is down/powerd off this time. MGCP application itself will failover immediately, so does the backhaul link. However as the backhaul link's status was not updated as the TCP layer is still in CLOSEWAIT, the backhaul link is in a false OPEN status and CCM will not be able to leverage this gateway to make outbound calls and all incoming calls are being impacted as well.

- CSCtu36446

Symptoms: The following error messages are displayed for the performance test with >20 CPS using the Cisco Radclient callsPerSecond Tool:

```
%FMANRP_ESS-4-SESSCNT: ESS Provision Lterm Session: Unsupported peer_segtype= (0x15)
%FMANRP_ESS-4-WRNPARAM_U: Get Lterm Peer ESS Segtype: Unsupported Peer SEGTYPE= (21)
%FMANRP_ESS-4-WRNEVENT2: Ignoring Invalid ESS Segment: ESS segment/signature (0x0 /
0x0)
%SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: Class ADJ: - unable to unbind
segment 2.
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[ADJ:Lterm:43232] - hardware platform error.
```

Conditions: This symptom is observed with high-scale, iEdge sessions.

Workaround: There is no workaround.

- CSCtu54300

Symptoms: Router crashes when you try to unconfigure the crypto.

Conditions: The symptom is observed when you clear the crypto and VRF configuration using automated scripts. The crash seen after the test is repeated three or four times. Before the crash the VRF and crypto features/functions are working fine.

Workaround: There is no workaround.

- CSCtw52819

Symptoms: OQD drops on mGRE tunnel.

Conditions: The symptom is observed with an mGRE tunnel.

Workaround: There is no workaround.

- CSCtw55401

Symptoms: The SPA-1XCHSTM1/OC3 card goes to out of service after SSO followed by OIR.

Conditions: This issue is seen with the SPA-1XCHSTM1/OC3 card with Cisco 7600- SIP-200 combination.

Workaround: There is no workaround.

- CSCtw70298

Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

Workaround: There is no workaround.
- CSCtw76527

Symptoms: The crypto session stays in UP-NO-IKE state.

Conditions: This symptom occurs when using EzVPN.

Workaround: There is no workaround.
- CSCtw79171

Symptoms: Platform asserts at adjmgr_l2_create.

Conditions: This symptom occurs with excessive flapping of a link.

Workaround: There is no workaround.
- CSCtw87132

Symptoms: A Cisco router may crash when clearing a TCP session:

```
router120#clear tcp tcb 08C5F4F8 [confirm]
SIGBUS (0xFF1BD460) : Bus Error ( [0xD0D0D39] invalid address alignment)
```

Conditions: This has been experienced on a Cisco 2921 router that is running Cisco IOS Release 15.1(4)M through to Release 15.1(4)M3.

Workaround: There is no workaround.
- CSCtw98200

Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.

Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS. RIP is configured with the **timers basic 5 20 20 25** command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise 5** command. These interfaces include the loopback and virtual-template interfaces too.

On a Cisco ASR1000 series router, this configuration causes the creation of full VAIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA sub-interfaces can be created.

Workaround: Unconfigure the **timers rip** command.
- CSCtx05726

Symptoms: When creating a bulk number of traffic engineering tunnel interfaces on the router with option **tunnel mpls traffic-eng exp-bundle master**, the standby route processor crashes.

Conditions: This symptom is seen with a specific set of configurations which has creation of a large number of tunnel interfaces (scale number 1000) followed by creation of large number of master tunnels (scale number 1000). Copying such a configuration to the router causes this crash on the standby processor.

The tunnel interfaces which are created at the beginning of the configuration are added as members to the master tunnels in the later part of the configuration. During this phase of creation of the master tunnels and adding member tunnels, these tunnel interfaces go through a cycle of “create-delete-create”. When such a configuration is being synced to the standby route processor along with the resulting create-delete events, the standby processor crashes.

This point where crash happens is random and can happen during configuration of any of the master tunnels.

Workaround: There is no workaround. Once the standby reboots after the crash, the configurations on the active are synced to the standby and this sync does not cause any crash. Crash is only during the initial copy of the configurations to the router.

- CSCtx06018

Symptoms: Interface queue wedge is seen when performing WAAS performance test.

Conditions: The symptom is observed when performing WAAS performance test.

Workaround: Increase interface input queue hold size.

- CSCtx06801

Symptoms: Certain websites may not load or load very slowly when content-scan is enabled. Delays of up to 30 seconds or more may be seen.

Conditions: The symptom is observed when content-scan is enabled.

Workaround: Though not always, refreshing the page sometimes helps.

Further Problem Description: The problem is due to GET request being segmented. For example, a huge get request of 1550 may come from the client in two different packets such as 1460+90=1550.

- CSCtx06813

Symptoms: Installation fails, “rwid type l2ckt” error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

Conditions: The symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

Workaround: There is no workaround.

- CSCtx11598

Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

```
% CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure
```

This failure can cause the SPA to go to one of the following states:

- none
- standby reset
- down

This failure leads to unexpected system reload.

Conditions: This symptom is observed during router reload for 15-20 times.

Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx23593

Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwalk** command, but not in the router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB.

Conditions: This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running Cisco IOS Release 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in the customer network. This issue may also occur in other releases.

This issue typically occurs over a period of time due to create/delete of subinterfaces. It also occurs if the customer uses the **snmp ifmib ifIndex Persist** command, which retains ifIndices assigned to the @~@subinterfaces across router reload.

Workaround: There can be two workarounds where there is no fix present in the Cisco IOS code for this bug.

Workaround 1:

- Enter the show atm vc privileged EXEC command on the same device to obtain a complete list of all the VCs. Or
- Do the SNMPWALK suffixing the ifIndex of the interface to get the value.

```
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.2.1.2.1.2 | grep
"4/0.120"
IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif
IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3 |
grep 9.9.66.1.1.1.1.3.254 ==> Got no entry of ifindex here in complete snmpwalk
$
```

```
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3.254
```

Doing the SNMPWALK suffixing the ifindex and getting the value can be one workaround.

```
SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041
```

Workaround 2:

1. Under configuration mode: no snmp ifmib ifIndex Persist.
2. On all the ATM main interfaces: no snmp ifindex persist.
3. Save the configuration: copy running start.
4. Reload the box: reload. Reapply the persist configurations.
5. Configure in configuration mode: snmp ifmib ifIndex Persist.
6. Under the ATM main interface: snmp ifindex persist.

After this workaround, the problem may reappear over a period of time, but chances are less.

The workaround/fix which needs to be enabled where the code fix is present in the Cisco IOS code for this bug.

Since this will go over all the possible ifIndices, it will take more CPU cycles, causing some delay. The below global CLI can be used to enable/disable the fix based on the need.

```
CLI: snmp-server enable traps atm snmp-walk-serial
```

- CSCtx32527

Symptoms: The **show crypto session** command reveals the flexVPN GRE tunnel is in a DOWN state instead of DOWN-negotiating.

Conditions: The symptom is observed with “ip address negotiated” configured on the GRE tunnel interface (with tunnel protection). The tunnel is unable to reach the gateway initially.

- Workaround: Configure an IP address on the tunnel interface instead of “ip address negotiated”.
- CSCtx34823
Symptoms: OSPF keeps on bringing up the dialer interface after idle-timeout expiry.
Conditions: This symptom occurs when OSPF on-demand is configured under the dialer interface.
Workaround: There is no workaround.
 - CSCtx36095
Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.
Conditions: This symptom occurs during a line card reload.
Workaround: There is no workaround.
 - CSCtx38121
Symptoms: IPv6 traffic is not passing through the interface attached with service policy matching IPv6 traffic using IPv6 ACL.
Conditions: This symptom is observed when attaching a service policy matching IPv6 traffic that is configured using ipv6 access-list on EFP of an interface, which will lead to a traffic drop.
Workaround: There is no workaround.
 - CSCtx40818
Symptoms: Traffic drops in a Cisco and displays the following error message:

```
%IP-3- LOOPPAK: Looping packet detected and dropped - src=122.0.0.11, dst=121.0.0.11, hl=20, tl=40, prot=6, sport=80, dport=57894
```


Conditions: This symptom is observed if the WAAS, NAT and firewall are enabled.
Workaround: Disable WAAS.
 - CSCtx48753
Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4/3.5.
Conditions: The symptom is observed with configurations with PPP sessions. These will see up to 10% higher IOS memory usage than in previous images.
Workaround: There is no workaround.
 - CSCtx54882
Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak.
Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.
Workaround: There is no known workaround.
 - CSCtx62138
Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.
Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.
Workaround: There is no workaround.
 - CSCtx66046
Symptoms: The Standby RP crashes with a traceback listing db_free_check.

Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

Workaround: Before removing the address, remove the network statement which covers the address of the loopback interface.

- CSCtx67028

Symptoms: Tracebacks are seen during a traffic condition when DMVPN and WAAS Express are configured.

Conditions: This symptom is observed while initiating an FTP session from the GW, where GW DMVPN and WAAS Express are configured.

Workaround: There is no workaround.

- CSCtx77501

Symptoms: Traffic is dropped at decap side of PE box.

Conditions: This symptom occurs with SSO at decap side of MVPN set-up, DFC core-facing, 6748 access facing.

Workaround: Do a switchover.

- CSCtx77750

Symptoms: Crosstalk may be heard by PSTN callers when a call is placed on hold and Music on Hold (MMOH) is enabled.

Conditions: CUCM is configured to do Multicast MoH.

Workaround:

1. Disable H.323 Multicast MoH functionality in IOS or use SIP Multicast MoH.
2. Use Unicast MoH

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 4.3/4.1:

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

CVE ID CVE-2012-1361 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

- CSCtx79462

Symptoms: OSPF neighborship does not get established.

Conditions: This symptom is observed when Enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx80535

Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

Conditions: PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

Workaround: Clear both sessions sharing the same IP.

- CSCtx92802

Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

Conditions: The symptom is observed under the following conditions:

- Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
- VRF enabled.
- CEF enabled.
- VPN tunnel.

Workaround: Disable VFR or CEF.

- CSCtx95840

Symptom: A Cisco voice gateway may unexpectedly reload.

Conditions: A Cisco voice gateway running SIP protocol. The crash stems from a timing issue in which a CCB data structure is freed prematurely while still in use.

Workaround: There is no workaround.

- CSCty01237

Symptoms: The router logs show:

```
<timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED  
CMD: 'show run' <timestamp>
```

This is followed by the router crashing.

Conditions: This issue is seen under the following conditions:

1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

Workaround 1: If you use PfR learn-list feature, do not execute **show run** periodically.

Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty03133

Symptoms: Memory leak in IPsec key engine process.

Conditions: The symptom is observed with the following conditions:

- Scale 1000 IKE * 1 Vrf * 4 IPsec, total 4K IPsec sessions.
- Multi-SA enabled.
- CAC=50,DPD=60 periodic.
- ~10M bidirectional traffic.

Workaround: There is no workaround.

- CSCty03745

Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

Conditions: This symptom occurs when the IPv4 default route exists, that is:

```
ip route 0.0.0.0 0.0.0.0 <next-hop>.
```

Or a certain static/IGP route exists: For example:

```
ip route 0.0.253.0 255.255.255.0 <next-hop>.
```

Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

```
router bgp 65000
  address-family l2vpn vpls
    neighbor 10.10.10.10 next-hop-self
```

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.
- CSCty05092

Symptoms: EIGRP advertises the connected route of an interface which is shut down.

Conditions: This symptom is observed under the following conditions:

 1. Configure EIGRP on an interface.
 2. Configure an IP address with a supernet mask on the above interface.
 3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

Workaround 1: Remove and add INTERFACE VLAN xx.

Workaround 2: Clear ip eigrp topology x.x.x.x/y.
- CSCty12312

Symptoms: Multilink member links move to an up/down state and remain in this condition.

Conditions: This symptom occurs after multilink traffic stops flowing.

Workaround: Remove and restore the multilink configuration.
- CSCty12524

Symptoms: BRI packet from LMA is not handled properly on MAG and also MAG is not sending the APN and SSMO option in PBRA.

Conditions: The symptom is observed on the originating or old MAG while clearing sessions in LMA in response to mobile node roaming to a new MAG.

Workaround: There is no workaround.
- CSCty17288

Symptoms: MIB walk returns looping OID.

Conditions: The symptom is observed when a media mon policy is configured.

Workaround: Walk around CiscoMgmt.9999.
- CSCty26685

Symptoms: A Cisco ASR 901 router may hit the rate limiting to cause a timeout.

Conditions: This symptom is seen when doing the inband TFTP download.

Workaround: Use the Cisco ASR901 management interface.

- CSCty27927
Symptoms: Bandwidth remaining percent on specific ports behave as rate limiters.
Conditions: This symptom is observed on specific ports, mostly g0/8.g0/9 and g0/10.
Workaround: Use other ports.
- CSCty29122
Symptoms: TCP TLS handshake fails for secure RTP calls.
Conditions: The symptom is observed with Cisco IOS interim Release 15.2(03.1)T.
Workaround: There is no workaround.
- CSCty35134
Symptoms: Data traffic out of REP EdgeNoNeighbor fails to flow.
Conditions: This symptom is observed when MST runs on the node when “rep stcn stp” is configured. If the MST puts this port to BLK then REP EdgeNN stops forwarding traffic.
Workaround: When having “rep stcn stp” configured on the rep port, we should not have a topology such that MST puts this port to blocking.
- CSCty35726
Symptoms: The following is displayed on the logs:
InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS
Conditions: This symptom is seen when video Xcode call with plain audio fails.
Workaround: There is no workaround.
- CSCty43587
Symptoms: Crash observed with memory corruption similar to the following:
%SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
dealloc XXXXXXXX
Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.
Workaround: There is no workaround.
- CSCty48870
Symptoms: Router crash due to a bus error.
Conditions: This has been observed in router that is running Cisco IOS Release 15.2(2)T and 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.
Workaround: Using **no ip nat service nbar** will help where NBAR is enabled through NAT.
- CSCty51453
Symptoms: Certificate validation using OCSP may fail, with OCSP server returning an “HTTP 400 - Bad Request” error.
Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T2 and later.
Workaround 1: Add the following commands to change the TCP segmentation on the router:
router(config)# ip tcp mss 1400
router(config)# ip tcp path-mtu-discovery
Workaround 2: Use a different validation method (CRL) when possible.

- CSCty53243

Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image sr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.

Workaround: There is no workaround.
- CSCty53923

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

Conditions: This symptom is observed when the nPE is the Cisco ME 3600X switch or the Cisco ME 3800X switch and the Standby Spoke VC terminates on it.

Workaround: There is no workaround.
- CSCty55449

Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

Conditions: If the policy uses the multiple event feature and the trigger portion is registered without curly braces (“{}”), then the device will crash. For example, this policy will trigger a crash:

```

::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger
::cisco::eem::correlate event 1 or event 2
namespace import ::cisco::eem::*
namespace import ::cisco::lib::*
action_syslog priority crit msg " triggered "

```

Note how “::cisco::eem::trigger” is not followed by an opening curly brace.

Workaround: Ensure that the trigger portion (i.e.: the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

```

::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger {
::cisco::eem::correlate event 1 or event 2 }
namespace import ::cisco::eem::*
namespace import ::cisco::lib::*
action_syslog priority crit msg " triggered "

```
- CSCty56850

Symptoms: Routers are not updating the cnpdAllStatsTable with traffic from all expected protocols.

Conditions: The symptom is observed with routers that are running Cisco IOS 15.x (tested in 15.0, 15.1 and 15.2(2)T).

Workaround 1: Use the following CLI to get the stats for all the protocols:

show IP NBAR protocol-discovery

Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.
- CSCty58992

Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

Conditions: This symptom is observed under the following conditions:

 - Cluster is in v6 mode.

- A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3 (SIP POTS), which is when the issue occurs.

Workaround: There is no workaround.

- CSCty59891

Symptoms: On the node where shut/no shut is issued, traffic does not reach IPsec VSPA, which is supposed to get encrypted.

Conditions: This symptom is observed when issuing shut/no shut on the GRE tunnel protected with IPsec and QoS configured on this IPsec tunnel.

Workaround: Remove and attach “tunnel protection ipsec profile”.

- CSCty61216

Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.

Conditions: The symptom is observed with the following IOS image:
c5350-jk9su2_ivs-mz.151-4.M2.bin.

It is seen with an outgoing SIP call from gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

Workaround: There is no workaround.

- CSCty63868

Symptoms: CUBE crashes at sipSPICheckHeaderSupport.

Conditions: CUBE crashes while running the codenomicon suite.

Workaround: There is no workaround.

- CSCty64216

Symptoms: On unconfiguring a scaled ACL, the router crashes.

Conditions: This symptom is observed when an ACL having 1000 ACEs or more is unconfigured.

Workaround: There is no workaround.

- CSCty71843

Symptoms: Tracebacks observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.

Conditions: The symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This is observed when a router is reloaded with the L2VPN configurations.

Workaround: There is no workaround.

- CSCty74859

Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

Conditions: The symptom is observed when ISG sessions are coming up on an HA setup.

Workaround: There is no workaround.

- CSCty76106

Symptoms: Crash is seen after two days of soaking with traffic.

Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

Workaround: There is no workaround.

- CSCty78435

Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty80553

Symptoms: Multicast router crashes.

Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCty83357

Symptoms: ACL denied packets are getting punted to host queue, leading to flaps in routing protocols.

Conditions: This symptom occurs when ACL is configured with src IP match, and packets are being denied by the ACL. The packets are punted to the CPU.

Workaround: There is no workaround.

- CSCty83520

Symptoms: IP Phone -- CUCM --- H323 -- 3845 - PSTN

1. A call is originated from the IP phone to a PSTN number and it gets connected.
2. The IP phone puts the call on hold.
3. The CUCM instructs GW to listen to the Multicast MoH stream.
4. The Cisco IOS Gateway sends the RTCP packet to Multicast MoH.

Conditions: This symptom is observed when the H.323 Gateway is configured and the Multicast MoH and MoH stream is sent across an IP Multicast network.

Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS.

Workaround 2: Use Unicast MoH.

- CSCty85926

Symptoms: VC (VPLS/EoMPLS) will stay down with the following in the **show mpls l2 vc detail** command:

Signaling protocol: LDP, peer unknown

Conditions: This symptom will only happen if you have LDP GR configured. Do a SSO switchover and try configuring the VC after the switchover is complete.

Workaround: There is no workaround. Reload the switch.

- CSCty86111

Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

Conditions: This symptom is observed with Cisco ISR G2 router.

Workaround: There is no workaround.

- CSCty90223

Symptoms: A crash occurs at `nhrp_nhs_recovery_co_destroy` during setup and configuration.

Conditions: This symptom is observed under the following conditions:

1. Add and remove the `ip nhrp` configuration over the tunnel interface on the spoke multiple times.
2. Do `shut/no shut` on the tunnel interface.
3. Rapidly change IPv6 addresses over the tunnel interface on the spoke side and on the hub side multiple times.
4. Replace the original (correct) IPv6 addresses on both the spoke and the hub.
5. Wait for the registration timer to start.

The crash, while not consistently observed, is seen fairly often with the same steps.

Workaround: There is no known workaround.

- CSCty91465

Symptoms: Ping to a global IP address (interface not part of any VRF) received via a VRF interface does not work even when “`vrf receive`” and the policy maps are configured correctly to receive the packets from the VRF interface.

Conditions: The symptom is observed when CEF is enabled.

Workaround: Disable CEF.

- CSCty94289

Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96049

Cisco IOS Software contains 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 single DHCP packet to or through an affected device, causing the device to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp>

- CSCty96052

Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty97784

Symptoms: The router crashes.

Conditions: This symptom is observed when NBAR is enabled, that is, “match protocol” actions in the QoS configuration, or “ip nbar protocol-discovery” on an interface or NAT is enabled and “ip nat service nbar” has not been disabled.

Workaround: There is no workaround.

- CSCty99874

Symptom: Ingress policing is done on the EVC which does not have QoS policy.

Conditions: This symptom is observed when one EVC has a QoS policy, and another does not. The QoS policy shows effect on the other EVC also.

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

- CSCtz00430

Symptoms: The static route is removed from the routing table.

Conditions: This symptom is observed when pulling out and replacing a connection to the management interface.

Workaround 1: Default the management interface and reconfigure IP.

Workaround 2: Do a shut and no shut on the management interface through the CLI.

- CSCtz02622

Symptoms: FlexVPN spoke crashed while passing spoke to spoke traffic.

Conditions: Passing traffic from spoke to spoke or clearing IKE SA on the spoke

Workaround: There is no workaround.

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 6.1/5:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-3893 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

- CSCtz03559

Symptoms: MVPN is seen on the Cisco ME 3600X and ME 3800X switches.

Conditions: This symptom is observed as currently, there are two SDM templates present in the Cisco ME 3600X and ME 3800X switches. Both templates do not support MVPN. A new SDM template is needed on the license “AdvancedMetroIPAccess” to support the MVPN.

Workaround: MVPN cannot be used without the new SDM template.

- CSCtz06611

Symptoms: IPSec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

Conditions: This symptom is a timing issue. You may see it first time or need to try multiple times. This symptom is seen with crypto map plus vrf configuration.

1. Reload the router with above configuration: the mac-address changes to all FF.
2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF.
3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

Workaround 1: Remove and add “ip vrf forwarding” and then remove and add the **crypto engine** command.

Workaround 2: Remove and add the **crypto engine** command.

Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08719

Symptoms: With split horizon, traffic does not flow on all BDs.

Conditions: This symptom is observed when traffic does not flow on all BDs.

Workaround: There is no workaround.

- CSCtz12714

Symptoms: A Cisco router configured for voice functions may crash.

Conditions: The exact conditions to trigger the crash are unknown at this time.

Workaround: There is no workaround.

- CSCtz13465

Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

Conditions: This symptom is observed with an interface with a policy installed.

Workaround: There is no workaround.

- CSCtz14980

Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.

Conditions: The symptom is observed when you have “crypto map GETVPN_MAP gdoi fail-close” configured and image is Cisco IOS XE Release 3.6 or 3.7.

Workaround: There is no workaround.

- CSCtz15211

Symptoms: The ISM card does not encrypt packets through a double encrypted tunnel.

Conditions: This symptom is observed with ISR g2 with the ISM module and crypto configured for GRE over IPsec packets to be encrypted through a VTI (double encryption).

Workaround: Use onboard encryption.

- CSCtz15274

Symptoms: When attempting a T.38 fax call on gateway, you may see the following in the logs:

```
006902: %FLEXDSPRM-3-UNSUPPORTED_CODEEC: codec cisco is not supported on dsp 0/0
006903: %FLEXDSPRM-5-OUT_OF_RESOURCES: No dsps found either locally or globally.
```

Conditions: The symptom is observed with a T.38 fax call.

Workaround: There is no workaround.

- CSCtz16622

Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.

Conditions: This symptom is seen with label pop action at the Edge-LSR.

Workaround: There is no workaround.

- CSCtz17977

Symptoms: Not able to ping HSRP VIP address over Routed VPLS.

Conditions: Two Cisco ME 3600s (me360x-universalk9-mz.152-2.S.bin) are connected together via VPLS. The Cisco ME 3600X-1 is configured with HSRP under VLAN50, and the R1 is able to ping. The R2 and Cisco ME 3600X-2 are not able to ping the VIP (HSRP) address. The R2 and Cisco ME 3600X-2 are able to ping physically the IP address of R1 and the Cisco ME 3600X-1. We do have ARP entry for the VIP address on all routers.

```
-----VPLS-----
R1 (fa0/1)-----Vlan50 ME3600X-1-0/2-----Ten-----0/2- ME3600X-2-Vlan50--
-----fa0/1-R2
```

Workaround: There is no workaround.

- CSCtz21456

Symptoms: A router has an unexpected reload due to CCSIP_SPI_CONTROL process.

Conditions: This issue has been seen in Cisco IOS Release 15.2(3)T.

Workaround: There is no workaround.

- CSCtz22112

Symptoms: A VXML gateway may crash while parsing through an HTTP packet that contains the “HttpOnly” field:

```
//324809//HTTPPC:/httpc_cookie_parse: * cookie_tag=' HttpOnly'
//324809//HTTPPC:/httpc_cookie_parse: ignore unknown attribute: HttpOnly
Unexpected exception to CPU: vector D, PC = 0x41357F8
```

Note: The above log was captured with “debug http client all” enabled to generate additional debugging output relevant to HTTP packet handling.

Conditions: The symptom is observed when an HTTP packet with the “HttpOnly” field set is received.

Workaround: There is no workaround.

- CSCtz23433

Symptoms: ISG shell maps with policer on egress child default-class fail.

Conditions: This symptom is seen with shell map with policer or shaper on child default-class.

Workaround: There is no workaround.

- CSCtz24047

Symptoms: Free process memory is being depleted slowly on line cards in the presence of the DLFioATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the show memory proc stat history command to display the history of free process memory.

Conditions: Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has Deflating configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

Workaround: There is no workaround.

- CSCtz25953

Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

Workaround: There is no workaround.

- CSCtz26188

Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds, then packets might be lost on the platforms where the forwarding updates take longer.

Workaround: Configure the value of the cleanup timer to 300 seconds.

```
mpls traffic-eng reoptimize timers delay cleanup 300
```

- CSCtz27782

Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.

Conditions: This symptom occurs when interface is in OAM RLB slave mode.

Workaround: There is no workaround.

- CSCtz28023

Symptoms: Traffic is not forwarded for a few mroutes.

Conditions: This issue is seen when multiple routers in the network are reloaded simultaneously.

Workaround: Using the **clear ip mroute vrf vrf name** command may resolve the issue.

- CSCtz30983

Symptoms: Crash on ES+ line card upon issuing the **show hw-module slot X tech-support** or **show platform hardware version** command.

Conditions: This symptom occurs on an ES+ line card.

Workaround: Do not issue the **show hw-module slot X tech-support** or **show platform hardware version** command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz31888

Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

Workaround: Increase the cost of access ring to more than 2M to avoid blocking of the BPDU PW.

- CSCtz33536

Symptoms: SIP KPML subscription fails with:

```
?xml version="1.0" encoding="UTF-8"?><kpml-response version="1.0" code="533"
text="Multiple Subscriptions on a Dialog Not Supported"/
```

This happens on a CUBE when the call is transferred on CUCM.

Conditions: The symptom is observed with SIP to SIP CUBE running Cisco IOS Release 15.1(3)T2.

Workaround: Use a different DTMF method.

- CSCtz34869

Symptoms: Aps-channel stops working.

Conditions: This symptom occurs with an open ring and is seen in the following scenario:

```
A1 (po2) (RPL) <=====> (po2) A3 (gig3/2) <=====> (gig3/3) A4
```

Shut down gig3/2 on A3. Does not make A1 into protection. => Debugs show no SF packets are being transmitted to A1 which is connected to A3 via “Port-channel” => A1 (po2) is RPL of the ring. It is not going to unblocked even after A3-A4 link goes down.

Workaround: Reload the line card.

- CSCtz35061

Symptoms: 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: There is no workaround.

- CSCtz35467

Symptoms: 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.

Conditions: 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.

- CSCtz37164

Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.

Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

Workaround: The fix is currently being worked upon. This issue can be seen as per the conditions mentioned above. This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz37863

Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

Conditions: The symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

Workaround: There is no workaround.

- CSCtz40621

Symptoms: Router crash observed.

Conditions: The symptom is observed when GetVPN GM tries to register to keyserver and keyserver issues a rekey simultaneously.

Workaround: There is no workaround.

- CSCtz40705

Symptoms: A configuration change which results in a serial interface being unconfigured (e.g. **no t1 channel channel-group channel-group-number**) may cause the router to reload if the serial interface is a xconnect member.

Conditions: This symptom has been observed when the **xconnect** command is configured on a channelized T1 serial interface with HDLC encapsulation and **no t1 channel channel-group channel-group-number** is configured to remove the channel group.

- Workaround: Remove the serial interface from the xconnect using the **no xconnect** command.
- CSCtz41048

Symptoms: The **trace mpls ipv4** command is unsuccessful.

Conditions: The symptom is observed with the **trace mpls ipv4** command.

Workaround: There is no workaround.
 - CSCtz43626

Symptoms: Minor or major temperature alarms reported in the syslog:

```
%C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold #1(=60C).
It has exceeded normal operating temperature range.
%C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
#1(=60C). It has exceeded normal operating temperature range.
```

Conditions: The symptom is observed on ES+ series line cards of Cisco 7600 series routers. Specifically, the reported temperature will be far off from reading of other sensors on the line card.

Workaround: There is no workaround.
 - CSCtz45057

Symptoms: High CPU is seen on a Cisco ME 3800X switch.

Conditions: This symptom occurs when loop of OTNIFMIB causes CPU Hog/Crash on a Cisco ME 3800X switch during pulling from PPM.

Workaround: Disable OTNIFMIB while pulling from PPM, which is not supported or required on Cisco ME 3800X and ME 3600X switches.
 - CSCtz45487

Symptoms: REP flaps when modifying allows VLANs on REP enabled trunk.

Conditions: This symptom is seen 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 Cisco IOS Releases 15.2(2)S, 15.1(2)EY2a and earlier Cisco IOS 15.1(2)S releases.
 - Issue is not seen on Cisco IOS Release 12.2(52)EY4 and earlier Cisco IOS 12.2(52)EY releases.

Workaround:

 - Remove “vlan dot1q tag native” global configuration.
 - Change to native VLAN 1 on the REP enabled trunks.
 - Change to Cisco IOS Release 12.2(52)EY.
 - CSCtz45901

Symptoms: The **show runn** or **format xml** output for an ATM interface is not displayed in the correct order.

Conditions: The symptom is observed if there are multiple subinterfaces for an ATM interface and PVC is configured under these.

Workaround: There is no workaround.
 - CSCtz47309

Symptoms: When using smart defaults in flexVPN, the mode transport may be sent from initiator even if “tunnel” is configured.

Conditions: First seen on a Cisco ASR that is running Cisco IOS Release 15.2(2)S and a Cisco ISR that is running Cisco IOS Release 15.2(3)T. It is seen with flexVPN.

Workaround: Use smart defaults on both sides on of the tunnel.

- CSCtz47873

Symptoms: The command **show crypto ikev2 client flex** does not work as expected.

Conditions: The symptom is observed with a client/server flexVPN setup.

Workaround: Execute either **show crypto IKEv2 sa** or **show crypto session detail**.

- CSCtz48615

Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

Conditions: The symptom is observed with AES encryption configuration in ISAKMP policy. The issue is seen only when one of the negotiating routers is a non-Cisco device where the key size attribute is not sent in ISAKMP proposal.

Workaround: Remove ISAKMP policy with AES encryption.

- CSCtz49200

Symptoms: OSPF IPv6 control packets are not encrypted/decrypted.

Conditions: This symptom is observed while configuring the IPv6 OSPF authentication.

Workaround: There is no workaround.

- CSCtz50204

Symptoms: A crash is observed on EzVPN Server if VRF configuration under the ISAKMP profile is modified.

Conditions: The crash is observed only if there are active sessions at the time of configuration change.

Workaround: Prior to applying a configuration change, clear the sessions.

- CSCtz59615

Symptoms: IPv6 route does not get installed in IPv6 VRF routing table.

Conditions: This symptom is seen in a Radius Framed-IPv6-Route.

Workaround: There is no workaround.

- CSCtz61599

Symptoms: After adding performance-monitor policy map under the port-channel interface, it displays continuously “Port-channel1 has more than one active member link”:

```
it-wan-agg5-14(config)#int port-channel 1
it-wan-agg5-14(config-if)#$performance-monitor input PERF-MON-port-channel
it-wan-agg5-14(config-if)#$performance-monitor output PERF-MON-port-channel
it-wan-agg5-14(config-if)#
Port-channel1 has more than one active member link
Port-channel1 has more than one active member link
```

Conditions: The symptom is observed after adding performance-monitor policy map under the port-channel interface.

Workaround: There is no workaround.

- CSCtz62680

Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

Conditions: When service policies less than 128 kb are added or removed.

Workaround: There is no workaround.

- CSCtz63438

Symptoms: In a GETVPN environment, the group member continuously registers to keyserver.

Conditions: The symptom is observed when the onboard crypto engine is disabled on a Cisco 1900 series platform.

Workaround: There is no workaround.

- CSCtz66770

Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

Workaround: Use aal5snap encapsulation.

- CSCtz67403

Symptoms: A Cisco ME 3600 switch as core switch is dropping all BPDU coming in QnQ tunnel.

Conditions: This symptom occurs on a Cisco ME 3600 switch that is the core, and the Cisco ME 3400 switches are edge switches.

Workaround: There is no workaround.

- CSCtz67726

Symptoms:

1. Single probe ID is not permitted on the **ip sla group schedule...** command. For example: **ip sla group schedule group id schedule-period 5 start now** gives following error messages:

```
%Group Scheduler: probe list wrong syntax %Group schedule string of probe ID's
incorrect
```

2. Entering the same probe ID under **ip sla group schedule** in the format of “id,id” is accepted but it will display on the running configuration as just single probe ID. For example: **ip sla group schedule group id,id schedule-period 5 start now**. The running configuration will show **ip sla group schedule group id schedule-period 5 start now**.

Conditions: Observed if using single probe ID under **ip sla group schedule...** command.

Workaround: Use the command **ip sla schedule** for single probe ID.

- CSCtz69084

Symptoms: The switch crashes when trying to enable IPsec MD5 authentication on the SVI.

Conditions: This symptom is observed with the following conditions:

```
VLAN 101
```

```
SW1-----SW2
```

1. Configure the IPsec MD5 authentication in global configuration mode.

```
ipv6 router ospf 1
```

```
area 0 authentication ipsec spi 1000 md5 123456ABCDEF123456ABCDEF123456AB
```

2. Configure the IPsec MD5 authentication as below in the interface mode with MD5 key 7 and device crashes.

Workaround: There is no workaround.

- CSCtz71084

Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

```
CE0-----PE0-----RR | | |
CE1-----PE1-----|
```

Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

Workaround: Hard clear.

- CSCtz72044

Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

Conditions: The issue is timing-dependent, therefore the problem is not systematic.

Workaround: There is no workaround.

- CSCtz72390

Symptoms: The name mangling functionality is broken. Authorization fails with the “IKEv2:AAA group author request failed” debug message.

Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

Workaround: There is no workaround.

- CSCtz72615

Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

Conditions: This symptom is observed on Cisco 7600 series routers.

Workaround: There is no workaround.

- CSCtz73157

Symptoms: CUBE sends 0.0.0.0 when 9971 has video enabled for hold/resume/conference from PSTN caller. CUBE sends correct IP address when 9971 has video disabled for hold/resume/conference from PSTN caller.

Conditions: The symptom is observed with the following conditions:

- Cisco IOS Release 15.2(2)T1.
- Current phone load sip99719.2.4-19.
- Current CUCM version: 8.5.1.13900-5.
- MCS7825I4-K9-CMD2A.

- On the SIP trunk, the box “Retry Video Call as Audio” was checked.

For the calls with video disabled, the CUBE is sending the 200OK with the C=IN ipX x.x.x.x address.

Sent:

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK7322e28fb58f2
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171271~17954349-bc2a-4081-adb4-34491012bb45-24984725
To: <sip:16464831236@x.x.x.x>;tag=D99A474-A1a
Date: Tue, 24 Apr 2012 18:26:17 GMT
Call-ID: f9e43000-f961f049-61593-a28050a@x.x.x.x
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 241
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 9798 5431 IN IPX x.x.x.x
s=SIP Call
c=IN IPX x.x.x.x
t=0 0
m=audio 25014 RTP/AVP 0 101
c=IN IPX x.x.x.x
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

For the calls with video enabled, the CUBE is not sending the IP address correctly, as seen here:

Sent:

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK734ab4c88ccb9
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171897~17954349-bc2a-4081-adb4-34491012bb45-24984949
To: <sip:16464831236@x.x.x.x>;tag=DA1D53C-2232
Date: Tue, 24 Apr 2012 18:35:25 GMT
Call-ID: 39f7e280-f961f262-616f4-a28050a@x.x.x.x
CSeq: 102 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Length: 278
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 144 2583 IN IPX x.x.x.x
```


- CSCtz78194
Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.
Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.
Workaround: Shorten the ISAKMP profile name to less than 31.
- CSCtz78943
Symptoms: A Cisco router experiences a spurious access or a crash. Cisco ISR-G1 routers such as a 1800/2800/3800 experience a spurious access. ISR-G2 routers such as the Cisco 2900/3900 routers that use a Power PC processor crash because they do not handle spurious accesses.
Conditions: This symptom occurs after enabling a crypto map on an HSRP-enabled interface. The exact conditions are being investigated.
Workaround: There is no workaround.
Further Problem Description: The CSCtx90408 DDTS was originally filed to fix this issue. Unfortunately, this caused another issue, which was addressed by backing out of the changes. The fix was backed out in the CSCty83376 DDTS, so this DDTS (CSCtz78943) will address both issues.
- CSCtz80643
Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive vrf name** command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.
Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive vrf name** command via the Virtual-Template or RADIUS profile.
Workaround: There is no workaround.
- CSCtz83221
Symptoms: Active or standby route processor crashes.
Conditions: This symptom can be seen during the configuration or removal of ATM virtual circuits.
Workaround: There is no workaround.
- CSCtz83311
Symptoms: In the bootlog, the following strings may be observed:

```
"MCB timeout"
```

Occasionally these messages also are followed by a GigE port link down for any of the ports Gig 0/1-Gig 0/8. A **shut/no shut** may not recover the link down condition.
Conditions: This symptom happens during a system reload. It may also happen if a **media-type** command is issued to the first eight GigE ports.
Workaround: Do not configure "media-type rj45" for the first eight ports either at bootup time or configurations if you are using an image that does not have this fix.
- CSCtz85907
Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now if "address-family ipv6" is configured under the VRF definition, MVPN traffic might be affected.
Conditions: This symptom is observed on Cisco IOS Release 12.2(33)SREx and RLSx releases.
Workaround: Use ingress replication.

- CSCtz86024
Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.
Conditions: This symptom is seen when there is no (*,G) on the box, and the first packet for the stream creates this entry.
Workaround: With static joins we can make sure that entry is present in mroute table.
- CSCtz86747
Symptoms: Router crashes upon removing all the class-maps from policy-map.
Conditions: This symptom is observed when a route crashes while removing all user defined class-maps with live traffic.
Workaround: Shut the interface first before removing class-map.
- CSCtz86763
Symptoms: Sessions remain partially created, and memory is consumed and not returned.
Conditions: This symptom occurs when sessions are churned and reset before they reach active state.
Workaround: There is no workaround.
- CSCtz87622
Symptoms: MLDP traffic is dropped for a few minutes a couple of times after SSO.
Conditions: This issue is seen soon after performing SSO.
Workaround: There is no workaround.
- CSCtz88289
Symptoms: It is observed that in a Cisco ME 3600-24CX unit, which is subjected to 100 consecutive image reloads, there is a system bootup hang in this area. The system stalls indefinitely and does not respond to console keystrokes like break keys.
<bootup snip>

```
I2C Bus Initialization begins
Margining CPU and Nile board Voltages
Control FPGA Initialization begins <<<<System Hang here
```


Conditions: This symptom may happen during a system bootup.
Workaround: A powercycle is required, and the next reload may not hit the above condition.
- CSCtz89608
Symptoms: A router that is operating in an ISG environment experiences a crash due to memory corruption.
Conditions: This symptom occurs within the SSS context.
Workaround: There is no workaround.
- CSCtz90909
Symptoms: A router crashes while giving the **no l2 vfi vfi-name point-to-point** command.
Conditions: This symptom occurs while unconfiguring l2 vfi. The router crashes.
Workaround: There is no workaround.

- CSCtz92606

Symptoms: MFR memberlinks-T1 serial interfaces created under a CHOC12 controller, do not get decoupled from MFR even after the MFR bundle interface is deleted. Once the MFR bundle interface is reconfigured, the memberlinks do not appear under it.

Conditions: This symptom is seen with MFR with memberlinks as T1 serials from CHOC12 sonet controller.

Workaround: Unconfigure and reconfigure the “encap frame-relay MFRx” under each memberlink after reconfiguring the MFR bundle interface.
- CSCtz94188

Symptoms: With AdvancedMetroIPAccess evaluation license and with TDM permanent license xconnect under CEM, ckts are not shown and are not configurable.

Conditions: This symptom occurs under regular configuration steps.

Workaround: There is no workaround.
- CSCtz94902

Symptoms: Memory allocation failure occurs when attaching to SIP-40 using a web browser.

Conditions: This symptom occurs on the line card.

Workaround: Reset the line card.
- CSCtz96167

Symptoms: QoS DSCP cases failing.

Conditions: The symptom is observed with a QoS profile (with DSCP as 31 configured under SBE) is being hit but DSCP bit is still sent as 0.

Workaround: There is no workaround.
- CSCtz96342

Symptoms: Inconsistency in scaled feature license name between Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* and Cisco IOS Release 15.2(2)S:

 - Cisco IOS Releases 12.2(52)EY*/15.1(2)EY*
 - ScaledServices Cisco IOS Release 15.2(2)S
 - ScaledMetroAggrServices

Conditions: This symptom occurs with an upgrade from Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* to Cisco IOS Release 15.2(2)S release, which could impact the scalability feature in below ways:

 - If user already had permanent license before upgrade, it will now downgrade to Eval license.
 - New license for installing ScaledMetroAggrServices cannot be generated as the license tool does not support this feature name.

Workaround: Upgrade to Cisco IOS Release 15.2(2)S1.
- CSCtz96504

Symptoms: Some of the backup VCs are down after SSO.

Conditions: This symptom happens only on scale scenario, for example, by creating 500 primary and 500 backup VCs.

Workaround: The backup VCs can be brought to SB state by issuing the **clear xconnect peerid peerid of the PW vcid vcid** command, although it is not usually recommended.

- CSCtz97244
Symptoms: IPSLA Video Operation with VRF support sees no packets received at responder.
Conditions: This symptom occurs when no emulate CLI is specified with the input interface.
Workaround: Use the emulate CLI to specify the input interface that has access to the VRF.
- CSCtz97755
Symptoms: ES card crash and alignment tracebacks on SP are seen.
Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running.
Unconfiguring IPv6 unicast-routing will lead to this issue.
Workaround: There is no workaround.
- CSCtz98486
Symptoms: The Flexwan QoS Offered Rate is not updated.
Conditions: This symptom occurs when traffic is flowing properly in both pos interfaces, where the offered on the policy-map o/p is not updated.
Workaround: There is no workaround.
- CSCtz99916
Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.
Conditions: This symptom occurs when call legs are not handled in a proper IWF container.
Workaround: There is no workaround.
- CSCua01375
Symptoms: Certificate validation fails when CRL is not retrieved.
Conditions: This symptom occurs when the router is configured to use a VRF.
Workaround: Use certificate map to revoke certificates or publish CRL to an HTTP server and configure “CDP override” to fetch the CRL.
- CSCua01641
Symptoms: The router’s NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

```
RADIUS: Acct-Session-Id      [44] 10 "00000001"
RADIUS: Acct-Status-Type    [40]  6 Accounting-On
[7]
RADIUS: NAS-IP-Address      [4]  6 0.0.0.0

RADIUS: Acct-Delay-Time     [41]  6 0
```

Conditions: Occurs when you restart the router.
Workaround: There is no workaround.
- CSCua03201
Symptoms: If the VPN ID of an existing Virtual Forwarding Interface (VFI) is changed on a dual-RP system, and then a stateful switchover (SSO) is performed, the new standby router may repeatedly reload.
Conditions: This symptom has been observed in Cisco IOS Release 15.2(2)S, Cisco IOS Release XE 3.6.0S, and later releases.
Workaround: In order to configure a new VPN ID for a VFI, completely remove the existing VFI and reconfigure it.

- CSCua04049

Symptoms: If a capture is stopped because of the limits reached and the capture is started immediately, the capture fails to stop.

Conditions: This symptom occurs after immediate activation of a capture.

Workaround: Clear buffer before activating the capture or wait for a minimum of 5 seconds before reactivation of a capture point.
- CSCua06476

Symptoms: When “clear crypto sa vrf” is executed to clear a non-GETVPN SA, there is an attempt to reregister the GETVPN group members irrespective of their data plane VRF.

Conditions: This symptom occurs when “clear crypto sa vrf” is executed to clear a non-GETVPN SA, and there is an attempt to reregister the GETVPN group members irrespective of their data plane VRF.

Workaround: There is no workaround.
- CSCua06598

Symptoms: Router may crash with breakpoint exception.

Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

Workaround: Disable SNMP IPv6 polling.
- CSCua07791

Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.

Conditions: The leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.

Workaround: There is no workaround.
- CSCua07927

Symptoms: MLDP traffic is dropped for local receivers on a bud node.

Conditions: This issue is seen on doing stateful switchover (SSO) on bud node.

Workaround: Using the **clear ip mroute vrf vrf name *** command for the effected VRFs will resume the MLDP traffic.
- CSCua08027

Symptoms: Tracebacks appear on a Cisco router when LI is used with SNMP based TAP. This happens with Cisco IOS Release XE 3.5S and later releases.

Conditions: This symptom is observed when SNMP based LI is used, and routers are running Cisco IOS Release XE 3.5S and later releases.

Workaround: There is no workaround.
- CSCua09073

Symptoms: If 6708 generates txCRC errors, these errors are accounted for in TestErrorMonitor diagnostic test and takes the necessary recovery action. The TestErrorMonitor test should be included in the test suite for 6708. This test is missing.

Conditions: For this fix to be take effect, TestErrorMonitor should be added in the test suite. In this DDTS, we are adding this test so that in case of an error, recovery action will be triggered.

Workaround: There is no workaround.

- CSCua10377

Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.
- CSCua12396

Symptoms: IPv6 multicast routing is broken when we have master switchover scenarios with a large number of members in stack. Issue is seen on platforms like Cisco 3750E and Cisco 3750X where IPV6 multicast routing is supported.

Conditions: This symptom is observed when IPV6 multicast routing is configured, mcast routes are populated and traffic is being forwarded. Now, in case of master switchover, synchronization between master and members is disrupted. This is seen only for IPv6 multicast routing. Observed the issue with 9-member stack and either during first or second master switchover. No issues are seen for IPv4 multicast routing.

Workaround: Tested with 5-member stack, and no issues are seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in stack.
- CSCua13322

Symptoms: Routes for the converted dedicated P sessions are missing after a RP switchover.

Conditions: This symptom occurs when converted dedicated IP sessions are not HA aware. After a RP switchover, these sessions will be reestablished at the new active RP. Routes are not installed for some of these sessions. As a result, downstream traffic is dropped.

Workaround: There is no workaround.
- CSCua13561

Symptoms: After upgrading to Cisco IOS Release 15.2(2)S, users cannot get IP address via PPP IPCP from DHCP pool on Cisco ASR router. There is no configuration change.

Conditions: This symptom occurs with an upgrade to Cisco IOS Release 15.2(2)S.

Workaround: Remove the **vpdn authen-before-forwardf** command.
- CSCua14594

Symptoms: Memory leak is seen when polling for the following PW MIBS:

```
1.3.6.1.4.1.9.10.106.1.5.1.1 (cpwVcPerfTotalInHCPackets)
1.3.6.1.4.1.9.10.106.1.5.1.2 (cpwVcPerfTotalInHCBytes)
1.3.6.1.4.1.9.10.106.1.5.1.3 (cpwVcPerfTotalOutHCPackets)
1.3.6.1.4.1.9.10.106.1.5.1.4 (cpwVcPerfTotalOutHCBytes)
```

Address	Size	Alloc_pc	PID	Alloc-Proc	Name
34417B84	308	13774B30	473	SNMP ENGINE	AToM VC event trace

This memory leak, on repeated polling, may lead to device crash.

Conditions: This symptom is observed with Cisco IOS Release 3.6S upon polling of the SNMP VC statistics query.

Workaround: There is no workaround.
- CSCua15003

Symptoms: When a call is canceled mid-call, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

Conditions: The problem can happen in the following situation:

- CUBE receives 180 ringing with SDP session.
- “media transcoder high-density” is enabled.

Workaround: Disable “media transcoder high-density”.

- CSCua16046

Symptoms: Some packets are dropped when multiple streams are merging on the Cisco ME 3600X and ME3800X switches. Sometimes, packet drops are seen with a single stream as well.

Conditions: This symptom is observed with smaller size packets such as 64-512 bytes.

Workaround: The workaround depends on the release. With some release, “no ip igmp snooping” will solve the issue.

- CSCua16786

Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua17746

Symptoms: IKEv2 with RSA-Sig as auth session will fail.

Conditions: The symptom is observed with:

- IKEv2 + RSA-Sig auth + ISM VPN; or
- IKEv2 + RSA-Sig auth + 7200 with VSA.

Workaround: Disable ISM VPN or VSA or do not use IKEv2 RSA-Sig as auth.

- CSCua17894

Symptom 1: On a Cisco ME 3600X and Cisco ME 3800X, a service policy that calls a class map with an empty or missing ACL will not get applied to an interface.

The switch will log the following:

```
QoS: Configuration failed. Can NOT allocate resources. --- or --- QoS: Policy
attachment failed for policymap <policy map name>
```

Symptom 2: A service policy is removed from an interface after a code upgrade from Cisco IOS Release 12.2(52)EY train to either Cisco IOS Release 15.2(2)S or Release 15.2(2)S1. On reload, the switch logs the following message:

```
QoS: Configuration failed. Can NOT allocate resources.
```

Conditions: The issue occurs if the service policy calls an ACL that does not exist or the ACL has only a “REMARK” statement but no entries.

Workaround: Ensure that the called access list is created prior to applying the policy map.

- CSCua19425

Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGp sessions with BFD configured between near end and far end routers.

Workaround: There is no workaround.

- CSCua21049

Symptoms: The recursive IPv6 route is not installed in the multicast RPF table.

Conditions: This symptom occurs in the multicast RPF table.

Workaround: There is no workaround.
- CSCua21166

Symptoms: Unable to form IPsec tunnels due to error:

```
''RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license.''
```

Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPsec from forming. Existing IPsec SAs will not be affected.

Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

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 2.8/2.3:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/RL:W/RC:C> No CVE ID has been assigned to 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
- CSCua21171

Symptoms: Ping will not pass between a few Distributed LFI over ATM (dLFIoATM) bundles.

Conditions: The symptom is observed after configuring a few dLFIoATM bundles. Check the ping between bundles and perform a shut/no shut of the interface.

Workaround: There is no workaround.
- CSCua21238

Symptoms: Cisco IOSd crashes at ipv6_address_set_tentative.

Conditions: This symptom occurs while unconfiguring IPv6 subinterfaces during the loading phase of a box with Netflow configuration.

Workaround: There is no workaround.
- CSCua24676

Symptoms: The VRF to the global packet's length is corrupted by -1.

Conditions: This symptom occurs when the next-hop in the VRF is global and recursive going out labeled. This issue is seen from Cisco IOS Release 15.0(1)S3a onwards, but is not seen in Cisco IOS Release 15.0(1)S2.

Workaround: Use the next-hop interface IP instead of the recursive next-hop.
- CSCua24689

Symptoms: Fragments are sent without label resulting in packet drops on the other side.

Conditions: The symptom is observed with the following conditions:

 - MPLS enabled DMVPN tunnel on egress.
 - VFR on ingress.

Workaround: Disable VFR if possible.

- CSCua25671

Symptoms: After adding the source interface in RSPAN, there is huge flooding to all trunks allowing RSPAN VLAN starts, even if there is no traffic on the RSPAN source interface.

Conditions: This symptom is observed under the following conditions:

1. The router has a RSPAN source session.
2. The source interface being added to the RSPAN source session is on ES+.
3. Any of the ES+ modules in the system has an interface on the RSPAN VLAN (that is, at least one of the interfaces on an ES+ module carries RSPAN replicated traffic).
4. The online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, are enabled on the ES+ module which has 2 and 3 mentioned above.

Workaround 1: Disable the online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, on the ES+ module which has the RSPAN source.

Workaround 2: If you have to use an interface on the ES+ module as a SPAN source, make sure that no other interface on any of the ES+ modules in the system is in the RSPAN VLAN. If you have to use an interface on the ES+ module to carry RSPAN replicated traffic, make sure that no other interface on any of the ES+ modules in the system is being monitored as an RSPAN source.

- CSCua25943

Symptoms: CPU Hog is observed on the LC when the number of IPv6 prefixes pumped in is more than 10,000.

Conditions: This symptom is observed when more than 10,000 IPv6 prefixes are pumped into the router.

Workaround: There is no workaround.

- CSCua26064

Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

Conditions: This symptom is seen when there are 4 core facing tunnels that load balance traffic to these prefixes. The **show mls cef ipv6 prefix detail** command shows the different adjacencies taken by different prefixes.

Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua27852

Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

Conditions: The symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR enabled.

Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua28346

Symptoms: A router crashes during second rekey.

Conditions: This symptom occurs with IKEv2 with RSA authentication.

Workaround: There is no workaround.

- CSCua29001

Symptoms: ANCP line rate is truncated on active-RP, but not on standby RP. As a result, the policy-map on the standby-RP will differ from that on active, and may fail to be applied.

Conditions: This symptom is seen when **ancp truncate value** CLI is enabled, and ANCP port ups are received on BRAS.

Workaround: There is no workaround.

- CSCua29095

Symptoms: Spurious memory access is seen when booting the image on a Cisco 7600 router.

Conditions: This symptom occurs while booting the image.

Workaround: There is no workaround.

- CSCua30053

Symptoms: Authentication is failing for clients after some time because the radius_send_pkt fails, because it complains about the low IOMEM condition.

Conditions: In AAA, minimum IO memory must be 512KB to process the new request. If the memory is less than this, AAA does not process the new authentication request. This is AAA application threshold. This application barriers are not valid in dynamic memory case. Such conditions are removed for NG3K platform.

Workaround: There is no workaround.

- CSCua30259

Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

Conditions: This symptom occurs when SPAN is configured on service instance.

Workaround: There is no workaround.

- CSCua31157

Symptoms: One way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.

Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly one minute after the tunnel between the spokes came up.

Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.

Workaround: There is no workaround.

- CSCua31794

Symptoms: After reload with the debug image, framed E1 lines are down.

Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “no-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua31903

Symptoms: IPv6 traffic is forwarded to wrong VRF when address is the same on both VRFs.

Conditions: This symptom is observed in an IPv6 MPLS VPN network that has PE routers, which have multiple CE routers connected. The CE routers are in different IPv6 VRFs. The CE routers have the same IPv6 address. The PE routers are dual and use dual stack. The problem happens on a 6VPE setup when the CEs share same the IP address.

Workaround: There is no workaround.

- CSCua31934
Symptoms: Crash seen at `__be_address_is_unspecified`.
Conditions: The symptom is observed with the following conditions:
 1. It occurs one out of three times and it is a timing issue.
 2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
 3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
 4. It can occur with v6 traffic alone.
 5. If you remove the tunnel interface on the Cisco ASR and add it again using **conf replace nvram:startup-config** the crash will occur.Workaround: Use CLI to change configuration instead of the rollback feature.
- CSCua32379
Symptoms: Cisco ASR 1000 hubs crash at `crypto_ss_set_ipsec_parameters`.
Conditions: The symptom is observed with dual-hubs switchover between active-standby and active-active.
Workaround: There is no workaround.
- CSCua33287
Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.
Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.
This condition will recover after executing **shut/no shut** on physical interfaces.
Workaround: There is no workaround.
- CSCua33527
Symptoms: Traceback seen after second or third switchover:

```
%LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
```


Conditions: The symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.
Workaround: There is no workaround.
- CSCua33821
Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.
Conditions: The symptom is observed after applying crypto maps.
Workaround: There is no workaround.
- CSCua34033
Symptoms: A Cisco ME 3800X hangs after boot.
Conditions: It is possible for an evaluation scaled license to be configured on the router and scaled services license configured. EULA acceptance can be ignored when configuring this. When the Cisco ME 3800X is rebooted, the router needs to program itself differently for a scaled license than a base license, but it cannot do so without the EULA being accepted so the router issues a prompt on the console port. The router will wait here until a user has responded. However, if a user is not on the console port to see this EULA message, they will not know that it is waiting for an EULA response. The router will continue to wait.

This is not seen on purchased licenses as they are not installed unless the EULA is accepted.

Workaround: When using evaluation licenses, accept the EULA upon configuring a license on the router or only reload the router from a connection to the console port after configuring the router to use an evaluation license.

- CSCua38881

Symptoms: Router reloads at clear_dspm_counter_per_bay.

Conditions: This issue is observed from Cisco IOS interim Release 15.2(3.16)M0.1 on Cisco 5350 and Cisco 5400 routers.

Workaround: There is no workaround.

- CSCua39390

Symptoms: The PRI configuration (voice port) is removed after a reload:

```
interface Serial1/0:23          ^
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
^
% Invalid input detected at '^' marker.
isdn incoming-voice voice
^
% Invalid input detected at '^' marker.
no cdp enable
^
% Invalid input detected at '^' marker.
voice-port 1/0:23
^
% Invalid input detected at '^' marker.
Also getting trace back
%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4. The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.

Workaround: Reapply configuration after router comes back up.

- CSCua40273

Symptoms: The Cisco ASR 1000 series router crashes when displaying MPLS VPN MIB information.

Conditions: Occurs on the Cisco ASR 1000 series router with Cisco IOS Release 15.1(2)S software.

Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua40369

Symptoms: DMM timestamping is not happening for IFM over EVC Xconnect and OFM over port-channel.

Conditions: DMM timestamping is not happening in the following conditions when:

1. Interface is used as core interface in EVC Xconnect.
2. Interface is used as a member in a port-channel.

- Workaround: There is no workaround.
- CSCua40790

Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

Conditions: This symptom occurs when BGPv4 neighbors are configured.

Workaround: There is no workaround if this MIB is to be polled.
 - CSCua41398

Symptoms: The SUP720 crashes.

Conditions: Occurs when you issue the `sh clns interface li ^[A-Z]` | Number of active command multiple times via script with following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012 pc=0x0 ,
ra=0x411514F4 , sp=0x55A8B080
c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC 0x41A78BB8
0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

Workaround: There is no workaround.
 - CSCua41464

Symptoms: Line card crash is seen while doing unconfiguration of mls rate limiters.

Conditions: This symptom occurs when the script configures 50 MVPN GRE VRFS, 50 MLDP VRFS, with 100 mroutes each. The crash happens when traffic is sent.

Workaround: There is no workaround.
 - CSCua42104

Symptoms: CUBE with a transcoder generates malformed RTCP packets.

Conditions: This symptom is observed with SIP-to-SIP CUBE with a transcoder registered to CUCM.

```
CIPC -- CUCM -- SIP -- CUBE -- SIP -- ITSP
CIPC -- G.729 -- CUBE (with transcoder) -- G.711 -- ITSP
```

RTCP packets sent from ITSP are sometimes malformed when CUBE them sends to the originating device.

Workaround: There is no workaround.
 - CSCua43930

Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

Conditions: The issue is seen on a Cisco ISR G2.

Workaround: There is no workaround.
 - CSCua44483

Symptoms: Mcast stops sending for all groups once all flows have ceased, due to timeout.

Conditions: This symptom occurs during normal operation, after senders have stopped sending and/or flows have timed out as normal.

Workaround: Disable and reenable mcast routing.

- CSCua45114

Symptoms: Default sessions will not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access interface. However the lite sessions are always brought up in the default VRF. If we need a lite session to not be in default VRF, move the interface to some access VRF.

Conditions: This symptom is seen when access-side interface is in the default VRF. The VRF is applied as a service to the default policy.

Workaround: There is no workaround.

- CSCua45548

Symptoms: Router crashes with **show ip sla summary** on longevity testing.

Conditions: The symptom is observed with Cisco 2900, 1900, and 3945 routers configured with IPSLA operations. The router which was idle for one day crashes on issuing the command **show ip sla summary**.

Workaround: There is no workaround.

- CSCua46304

Symptoms: A crash is seen at `__be_nhrp_group_tunnel_qos_apply`.

Conditions: This symptom is observed when flapping a DMVPN tunnel on the hub in a scale scenario.

Workaround: There is no workaround.

- CSCua47570

Symptoms: The **show ospfv3 event** command can crash the router.

Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.

Workaround: Do not use the **show ospfv3 event** command.

- CSCua48584

Symptoms: The Cisco ME 3600X’s ARP resolution may fail after flexlink switchover.

Conditions: This 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.

- CSCua48807

Symptoms: Complete traffic loss is observed.

Conditions: This symptom is observed when queue-limit and default WRED “random-detect” are configured in a class and dynamically modify queue- limit of that class.

Workaround: There is no workaround.

- CSCua49764

Symptoms: The WAAS-Express device goes offline on WCM.

Conditions: This symptom occurs when a certificate is generated using HTTPS when using the Cisco IOS Release 15.1(3)T image. Once upgraded to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.

Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the **enroll** command again or delete the self-signed trustpoint point and reenble the HTTP secure-server.

- CSCua52289

Symptoms: CPU hog is seen on the line card due to Const2 IPv6 process.

Conditions: This symptom occurs with 4 core facing tunnels. Upon FRR cutover, the CPU hog is observed.

Workaround: There is no workaround.

- CSCua52439

Symptoms: MLD reports are not received on ES+.

Conditions: This symptom is seen on sending MLD joins on ES+. The reports are not received on the router.

Workaround: There is no workaround.

- CSCua55691

Symptoms: A Cisco IOS memory leak is observed.

Conditions: This symptom is seen when unconfiguring/reconfiguring BGP AD VFIs.

Workaround: There is no workaround.

Further Problem Description: This issue is seen during longevity run.

- CSCua55752

Symptoms: Unexpected set IP next-hop will be applied on packets subjected to PBR. This happens only if similar next-hop is tracked with multiple tracking objects.

Conditions: This symptom occurs when PBR is applied on incoming interface and verify-availability tracking option is configured.

Workaround: Avoid configuring same next hop with multiple tracking objects.

- CSCua55797

Symptoms: The **privilege exec level 0 show glbp brief** command causes the memory to be depleted when the **show running** or **copy running-config startup-config** commands are used. The configurations will then show this:

```
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief brief
brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief brief
brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
privilege exec level 0 show glbp GigabitEthernet0/0 brief
privilege exec level 0 show glbp privilege exec level 0 show
```

Removing the configurations causes this to happen over and over until the telnet session is terminated:

```
priv_push : no memory available
```

If the configurations are saved and device is reloaded, the device will not fully boot until the configurations are bypassed.

Conditions: This issue happens after the **privilege exec level 0 show glbp brief** command is entered and saved.

Workaround: Reload the router before saving the configurations.

- CSCua56184

Symptoms: Multiple RP switchovers occur within a very short span of time.

Conditions: The symptom is observed with multiple RP switchovers on a Cisco ASR 1000 router and it fails to allocate an IPsec SPI.

Workaround: There is no workaround.

- CSCua56802

Symptoms: QoS will not work on one of the subinterfaces/EVC.

Conditions: This symptom occurs when HQoS policy is configured on more than one subinterface/EVC on ES+ and then add flat SG on them.

Workaround: Remove and reapply SG.

- CSCua57728

Symptoms: Traffic loss of ~25s is seen upon doing TE FRR Cutover with IPv6 prefixes.

Conditions: This symptom is observed with four core facing tunnels, and 100,000 IPv6 prefixes. Shut the primary interface and check for the traffic loss.

Workaround: There is no workaround.

- CSCua58100

Symptoms: The syslog is flooded with the following traceback message:

```
Jun 20 10:05:23.961 edt: %SYS-2-NOTQ: unqueue didn't find
7F3D26BDCCD8 in queue 7F3CA5E4A240 -Process= "RADIUS Proxy", ipl= 0, pid= 223
-Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812 :400000+873623 :400000+2547652
:400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
```

Conditions: Occurs under the following conditions:

- You establish 36k EAPSIM sessions using a RADIUS client on server A.
- You establish 36k roaming sessions using a RADIUS client on server B.
- The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

Workaround: There is no workaround.

- CSCua60395

Symptoms: When an IPv6 packet is received via EoMPLS pseudowire, the packet is punted to the CPU and sent back on the pseudowire.

Conditions: This has been identified on a Cisco ME3600X with Cisco IOS Release 15.2(1)S1.

Workaround:

Option 1: Configure the xconnect under a interface vlan and configure a (dummy) IP address.

Example:

```
interface vlan XXX
ip address A.B.C.D M.M.M.M
xconnect N.N.NN <vc-id> encapsulation mpls
```

Option 2: Block IPv6 packets on remote end so that these packets are not sent over pseudowire.

- CSCua61814
Symptoms: Overhead accounting configuration needs to be configured on both parent and child policy, rather than just parent.
Conditions: The symptom is observed with overhead accounting.
Workaround: There is no workaround.
- CSCua63182
Symptoms: Incorrect minimum bandwidth is displayed when 0k bandwidth is received from a peer of a different version.
Conditions: This symptom occurs under the following conditions:
 - Different behavior in Cisco ASR code when the bandwidth for a route is very high, that is, more than 10G.
 - Cisco IOS XE Release 2.6.2 and earlier releases send 0K when the bandwidth for a route is more than 10G.
 - Cisco IOS XE Release 2.6.2 and earlier releases use incoming interface bandwidth, when BW = 0 is received.
 - Cisco IOS XE Release 3.4.3S and later releases send the real bandwidth, even if it is more than 10G.
 - Cisco IOS XE Release 3.4.3S and later releases use the lesser value between “received bandwidth” and “incoming interface bandwidth”.
 - Cisco IOS XE Release 3.4.3S and later releases convert incoming bandwidth to 1K in case BW = 0 received.
 - When the peers are of the same or compatible version, that is, both peers are Cisco IOS XE Release 2.6.2 and earlier releases or both peers are Cisco IOS XE Release 3.4.3S and later releases, there is no issue. However, when the peers are of different or incompatible version, that is, one peer is Cisco IOS XE Release 2.6.2 or an earlier release and the other peer is Cisco IOS XE Release 3.4.3S or a later release, then this issue is seen.Workaround: There is no workaround.
- CSCua64546
Symptoms: In a scaled setup with IPV4 and IPV6 ACL together (not necessarily on the same interface), IPV4 ACLs may stop working if the IPV6 ACL configured later overwrites the IPV4 ACL results and vice versa.
Conditions: This symptom is observed with IPV4 and IPV6 ACLs configured on the box.
Workaround: There is no perfect workaround. Reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.
Further Problem Description: Only the IPV4 or IPV6 ACL configuration will work.
- CSCua64676
Symptoms: MVPNv4 traffic is not flowing properly from remote PE to UUT.
Conditions: This symptom is seen with Agilent traffic on and after removal/addition of MDT configs for the MVRFs configured on the UUT, MVPNv4 traffic is not flowing properly from remote PE to UUT.
Workaround: There is no workaround.
- CSCua64700
Symptoms: The IPsec tunnel state goes to Up-Idle after 4-5 days of the router being up and running.

Conditions: This symptom is observed if you have low rekey value, as with the rekey, the new SPI gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter.

```
show crypto ace spi
```

If there is no decrement in the SPI allocated counter and there is a consistent increment in the counter, the chances are high that you will encounter this issue.

Once the value reaches 61439, you will encounter this issue.

```
MTCVFNK03#sh cry ace spi SPI in use ..... 0 Normal SPI allocated
..... 61439
```

Workaround: There is no workaround. You need to reload the box.

- CSCua66908

Symptoms: Build fails on Cisco IOS Release 15.3M&T.

Conditions: This symptom was observed after the commit of CSCua06101 due to unnecessary duplication of a line.

Workaround: Remove the line before building.

- CSCua67532

Symptoms: IPsec sessions fail to come up.

Conditions: This symptom occurs when Site-Site crypto configuration using crypto map is applied on SVI, and when no ISAKMP profile is configured under that crypto map.

Workaround: There is no workaround.

- CSCua68243

Symptoms: IGMP and PIM control packets are not reaching RP. As a result, the mac-address table for IGMP snooping entries is not populated.

Conditions: This can be seen on a Cisco 7600 series router that is running IOS where IGMP and PIM control packets come in on an SVI only after the condition where the SVI link state goes down and comes up again. This does not affect routed ports.

Workaround: In the SVI configuration mode:

1. Unconfigure PIM by using **no ip pim**.
2. Unconfigure IGMP snooping by using **no ip igmp snooping**.
3. Re-enable both PIM and IGMP snooping.

- CSCua68398

Symptoms: The ES+ card crashes.

Conditions: This symptom is observed with a scaled EVC and VPLS configurations.

Workaround: Stop the traffic. After the line cards boot up and the ports are up, start the traffic.

- CSCua69657

Symptoms: Traceback is seen when executing the **show clock detail** command.

Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T image.

Workaround: There is no workaround.

- CSCua71038

Symptoms: Router crash.

Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

Workaround: Configure OCSP or CRL but not both

- CSCua75566

Symptoms: Scalable EoMPLS traffic drop is observed at disposition side after performing provision/unprovision of xconnect VCs.

Conditions: This symptom is occurs when scalable EoMPLS is configured between PE routers and AC is interface of ES+ model 76-ES+T+XC-40G, ES+ HD as core facing interface.

Workaround: There is no workaround.

- CSCua75781

Symptoms: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

Conditions: The symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

Workaround: There is no workaround.

- CSCua78468

Symptoms: Under a heavy load, L4F may not forward packets to the scansafe process. Unit may crash while trying to remove scansafe off the interface.

Conditions: This issue was first identified on a Cisco ISR running the 15.2.4 image.

Workaround: There is no workaround.

- CSCua80204

Symptoms: EoMPLS remote port shutdown feature does not work.

Conditions: This symptom is observed if xconnect and a service instance are configured under the same interface.

Workaround: There is no workaround.

- CSCua81998

Symptoms: Doing ISSU RV in a Cisco 7600 box with the ES40 line card may sometimes cause a crash in the ES40 line card.

Conditions: This symptom is seen with ISSU RV with Cisco IOS Releases XE 3.7S or XE 3.8s to XE 3.6.1S.

Workaround: There is no workaround.

- CSCua83876

Symptoms: Some multicast streams may stop being forwarded, or new multicast streams cannot be joined. In parallel the following message is displayed:

```
allocate_l3m_port_fcje: RPF PASS nh_hdl(0xD2668C0) MET FULL ERR
```

Conditions: This has been observed on a Cisco ME 3600X that is running Cisco IOS Release 15.2(2)S1.

Workaround: There is no workaround.

Further Problem Description: A reboot is required in order to clear the situation temporarily.

- CSCua84147

Symptoms: Router crashes during “sh run | format” CLI execution.

Conditions: This crash is seen only during “sh run | format” execution. All other CLI executions are fine.

Workaround: Avoid executing “sh run | format”. Instead “sh run” can be executed.

- CSCua84879

Symptoms: Crash at slaVideoOperationPrint_ios.

Conditions: The symptom is observed when IPSLA video operations are configured and **show running-config** is issued.

Workaround: There is no workaround.

- CSCua85239

Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller "mtu" or "ip mtu" configured.

```
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP
Notification sent
UTC: %BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0
(hold time expired) 0 bytes
%BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4
Unicast topology base removed from session BGP Notification sent
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
```

Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

- If the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
- Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

Workaround: There is no workaround.

- CSCua85837

Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua85934

Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

Conditions: This symptom is observed with the ISG-SCE interface.

Workaround: There is no workaround.

- CSCua86620

Symptoms: The vmware-view application is not detected/classified.

Conditions: This symptom is observed when vmware-view applications are used.

Workaround: There is no workaround.

- CSCua88341

Symptom: Multicast traffic on P2P GRE tunnel will get dropped.

Conditions: This symptom usually happens in scenarios like SSO, which is done after VRF deletion or addition. Here the P2P GRE tunnel will be in the VRF.

Workaround: Do a shut/no shut of the P2P GRE tunnel interface.

- CSCua91104

Symptoms: ISIS adjacency process shows traceback messaging related to managed timer.

Conditions: This symptom is seen when configuring isis network point-to-point on LAN interface with isis bfd or isis ipv6 bfd enabled. The traceback does not happen always. It depends on timing.

Workaround: Disable isis bfd or isis ipv6 bfd before issuing **isis network point-to-point** command. Restore isis bfd or isis ipv6 bfd configuration on LAN interface.

- CSCua91473

Symptoms: Memory leak occurs during rekey on the IPsec key engine process.

Conditions: This symptom occurs after rekey, when the IPsec key engine does not release KMI memory, causing the IPsec key engine holding memory to keep increasing.

Workaround: Clear crypto session for IPsec key engine to release memory.

- CSCua91698

Symptoms: ephone-type disappears from the running-configuration.

Conditions: This symptom occurs in SRST mode and after reload.

Workaround: Reconfigure the ephone-type commands and again save to startup-configuration.

- CSCua92741

Symptoms: Remote neighbors are denied by the allow-list to come up.

Conditions: This symptom occurs when the remote neighbor is configured with a /32 IP address.

Workaround: There is no workaround.

- CSCua94334

Symptoms: Hung calls are seen on CME. Hung calls seen in “show call active voice brief” are as follows:

```
1502 : 26 36329310ms.1 +-1 pid:1 Answer XXXYYY4835 connected
dur 00:00:00 tx:0/0 rx:0/0
IP 0.0.0.0:0 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8
pre-ietf TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

Conditions: This symptom is observed when an inbound H225 call setup request to a CME gateway results in a hung call if a release complete is received while still in alerting state. This issue occurs only when the shared line is configured on the phone and the shared line is not registered.

Workaround: Remove the shared line or register the shared line.

- CSCua94947

Symptoms: RP crashes when downloading FreeRadius Framed-IPv6-Route on MLPPP sessions.

Conditions: This symptom occurs when downloading radius Framed-IPv6-Route.

Workaround: There is no workaround.

- CSCua96354

Symptoms: Reload may occur when issuing the **show oer** and **show pfr** commands.

Conditions: This symptom is observed with the following commands:

- **show oer master traffic-class performance**
- **show pfr master traffic-class performance**

Workaround: There is no workaround.

- CSCua96392

Symptoms: HSRP stops working after shut/no shut on a port channel member.

Conditions: The issue is seen when a port-channel (with at least 2 members) member is shut.

Workaround: There is no workaround.

- CSCua98421

Symptoms: RMEPs from a Cisco ASR 9000 are not learned on a Cisco ME 3800X with CFM running over an xconnect. The Cisco ASR 9000 does learn the RMEPs from the Cisco ME 3800X.

Conditions: This symptom is seen when 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.

- CSCua98690

Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

Conditions: This symptom is observed when the MAC ACL is configured on EFP.

Workaround: There is no workaround.

- CSCua98902

Symptoms: fibidb is not getting initialized.

Conditions: This symptom is observed when LFA FRR is configured in Cisco ME 3800x and ME 3600x switches.

Workaround: There is no workaround.

- CSCub01494

Symptoms: AD in the route installed by client is not updated to the configured value.

Conditions: This symptom is seen when the CLI “ip route 0.0.0.0 0.0.0.0 dhcp 5” is configured. AD is not updated to 5.

Workaround: There is no workaround.

- CSCub05907

Symptoms: Reverse routes are not installed for an IPsec session while using dynamic crypto map.

Conditions: This symptom occurs when the remote peer uses two or more IP addresses to connect and it goes down and comes back at least twice.

Workaround: Issue “clear crypto session” for that peer.

- CSCub06131

Symptoms: The IPSLA sender box can reload with the following message:

SYS-6-STACKLOW: Stack for process IP SLAs XOS Event Processor running low, 0/6000
Conditions: This symptom is observed with the IPSLA sender box.

Workaround: There is no workaround.

- CSCub07382

Symptoms: NHRP cache entry for the spokes gets deleted on NHRP hold timer expiry even though there is traffic flowing through the spoke-to-spoke tunnel.

Conditions: The symptom is observed with a flexVPN spoke-to-spoke setup.

Workaround: Configure the same hold time on both tunnel interface and the virtual-template interface.

- CSCub07673

Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. “Volume rekey” is disabled on Zamboni.

Conditions: This symptom occurs if we have “volume rekey” disabled on Zamboni.

Workaround: Do not disable the volume rekey on Zamboni.

- CSCub07855

Symptoms: The VRF error message is displayed in the router.

Conditions: This symptom occurs upon router bootup.

Workaround: There is no workaround.

- CSCub08714

Symptoms: Poor performance for multicast on a Cisco ASR 1000 series router over dmvpn

Conditions:

1. Multicast packet has to be coming in on a Tunnel interface (not a physical interface).
2. NS (negate signaling) flag has to be set on one of the interfaces in the MFIB (S,G) entry.

If both these conditions are met, then the packet is punted to control plane & forwarded in software in addition to the hardware forwarding thus causing duplicates. Note that the NS punts are periodic/throttled and not all multicast packets are punted because of NS. Thus the duplication is intermittent/periodic.

Workaround: There is no workaround.

- CSCub09124

Symptoms: MDT tunnel is down.

Conditions: This symptom is seen in MVPN. If the **ip multicast boundary** command on non-current RPF interface blocks the MDT group, it may cause MDT tunnel failure.

Workaround: Adding the **static join** command under PE loopback interface may work around the problem temporarily.

- CSCub10951

Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

Conditions: This symptom is observed with the following conditions:

1. The following configuration exists at all RRs that are fully meshed:
 - bgp additional-paths select best-external
 - nei x advertise best-external

2. For example, RR5 is the UUT. At UUT, there is,
 - Overall best path via RR1.
 - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.
 - Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.
3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
4. At PE6, reconfigure the route so that RR5 will have “ic_path_rr5” as its “best-external (internal) path”. At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

Workaround: Hard/soft clear.

- CSCub14044

Symptoms: A crash with traceback is seen, and all calls are dropped.

Conditions: This symptom is observed under all conditions.

Workaround: There is no known workaround. The gateway crashes, and the soak time appears to be six weeks.
- CSCub14299

Symptoms: The router reloads when “no mediatrace initiator” is issued.

Conditions: This symptom occurs when traceroute is enabled for a mediatrace session.

Workaround: Disable traceroute under each configured mediatrace session.
- CSCub15542

Symptoms: Configuring mpls lsp trace results in IOSD restart.

Conditions: This symptom occurs when configuring mpls lsp trace results in IOSD restart.

Workaround: There is no workaround.
- CSCub17985

Symptoms: A memory leak is seen when IPv6 routes are applied on the per-user sessions.

Conditions: This symptom is seen if IPv6 routes are downloaded as a part of the subscriber profile. On applying these routes to the sessions, a memory leak is observed.

Workaround: There is no workaround.
- CSCub18997

Symptoms: A Cisco ME 3800 may crash after the following error message is displayed:

```
%SYS-6-STACKLOW: Stack for process Non-Qos Events Process running low, 0/6000
```

Conditions: This symptom is observed on a Cisco ME 3800 that is running Cisco IOS Release 15.2(2)S1.

Workaround: There is no workaround.
- CSCub21468

Symptoms: UDP header is corrupted randomly.

Conditions: This symptom is observed with the Cisco 7609-S (RSP720-3C-GE) running Cisco IOS Release 12.2(33)SRE5, with the VRF Aware LI feature.

Workaround: There is no workaround.

- CSCub24079
Symptoms: TAR bundle does not get downloaded through the **archive** command.
Conditions: This symptom applies to any conditions.
Workaround: Untar externally and copy to flash/ucode1 directories.
- CSCub25360
Symptoms: In a Flexlink switchover scenario, it seems that for some reason, the Cisco ME 3600X switch does not sent out a dummy Mcast packet for the SVI.
Conditions: This symptom is observed with a Cisco ME 3600X Flexlink switchover.
Workaround: There is no workaround.
- CSCub26079
Symptoms: Service policies are not getting applied on ATM interface.
Conditions: This symptom is observed when client is configured with “ppp chap hostname peer” and a PPOA session is established. Policies 7up and sprite are installed on interface of UUT. Later the client “ppp chap hostname Rate” is configured and that time policies are downloaded from radius, which have not replaced previous policies 7up and sprite.
Workaround: There is no workaround.
- CSCub31477
Symptoms: A Cisco ISG router configured for Layer 2 Connected Subscriber Sessions does not respond to ARP replies once a subscriber ARP cache has expired.
Conditions: This symptom occurs when the router is configured as ISG L2-Connect, the router has configured HSRP as the high-availability method, and the subscriber-facing interface is configured with “no ip proxy arp”. This issue is not seen if either HSRP is removed or if “ip proxy arp” is enabled.
Workaround: Clear the subscriber session. After the subscriber is reintroduced, the issue is resolved. You can also configure “ip proxy arp” on the HSRP-configured interface.
- CSCub31592
Symptoms: After the flap of the interface with EVC configured, box is no longer adding second tag to the traffic. Forwarding is broken. See the following example:

```
service instance 100 ethernet
  encapsulation dot1q 10
  bridge-domain 100
```


Conditions: This symptom is seen with the flap of the interface.
Workaround: There is no workaround.
- CSCub32500
Symptoms: The router crashes in EIGRP due to chunk corruption.
Conditions: This symptom is observed on EIGRP flaps.
Workaround: There is no workaround.
- CSCub33602
Symptoms: IGMP query with source IP address 0.0.0.0 triggers a querier election process. As a consequence, port on which this packet is received is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
Internet address is 1.1.1.1/24
```

```
IGMP querying router is 0.0.0.0 <----
```

```
Router#sh ip igmp snooping mrouter
vlan          ports
-----
```

```
1 Po1,Po8,Router<-----
```

Conditions: This symptom is seen when IGMP query with source IP address 0.0.0.0 is received.

Workaround: Configure an ACL to block packets with source IP address 0.0.0.0 and apply it to relevant interfaces.

```
access-list 100 deny ip host 0.0.0.0 any
access-list 100 permit ip any any
int vlan 1
ip access-group 100 in
```

Further Problem Description: Per RFC 4541, IGMP query with source IP address 0.0.0.0 is used in special cases. When such query is received by a router, it should not be used in the querier election process.

- CSCub33877

Symptoms: During “issue loadversion”, when downgrading from Texel (or later) to Yap (v151_1_sg_throttle or earlier), the standby RP keeps reloading due to the out of sync configuration.

Conditions: This symptom occurs during the “issu loadversion” operation. The newer version of the image supports IPv6 multicast while the older version of image does not.

Workaround: There is no workaround.

- CSCub34595

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

Conditions: This symptom is seen when enabling DAI on a VLAN.

Workaround: Enable DAI for the failing VLAN with the **ip arp inspection vlan x** command. Eg:

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

Workaround: Enable DAI for the failing VLAN with the **ip arp inspection vlan x** command.

Configure an ARP ACL to permit traffic for valid IP source + MAC source pair with the **arp access-list acl_name** command. Configure DAI filter and associate with the ARP ACL with the **ip arp inspection filter acl_name vlan x** command. Configure DAI trust on egress port with **ip arp inspection trust**. Eg:

```
ip arp inspection vlan 20
arp access-list testacl
permit ip 10.1.1.3 255.255.255.0 mac 01:00:00:0E:0E:0F
ip arp inspection filter testacl vlan 20
int gig0/10
ip arp inspection trust
```

- CSCub35388

Symptoms: The **port-channel min-links** command is rejected under port-channel.

Conditions: This symptom is seen when port-channel has a VRF configuration.

Workaround: Configure the **min-link** command and then configure the **vrf** command under port-channel.

- CSCub36217

Symptoms: When the Cisco ME3800 router is running Cisco IOS Release 15.2(4)S software, if EVC maximum MAC security address limit is reached for a service instance, new MAC address is not rejected.

Conditions: This symptom is seen when EVC MAC security is enabled under a service instance.

Workaround: There is no workaround.

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 1.7/1.3:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:L/Au:S/C:N/I:P/A:N/E:U/RL:OF/RC:C> No CVE ID has been assigned to 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

- CSCub39268

Symptoms: Cisco ASR 1000 devices running an affected version of IOS-XE are vulnerable to a denial of service vulnerability due to the improper handling of malformed IKEv2 packets. An authenticated, remote attacker with a valid VPN connection could trigger this issue resulting in a reload of the device. Devices configured with redundant Route Processors may remain active as long as the attack is not repeated before the affected Route Processor comes back online.

Conditions: Cisco ASR1000 devices configured to perform IPSec VPN connectivity and running an affected version of Cisco IOS-XE are affected. Only authenticated IKEv2 connection is susceptible to this vulnerability.

Workaround: There is no workaround.

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 6.8/5.6:

<https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C> CVE ID CVE-2012-5017 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

- CSCub39296

Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

Conditions: The symptom is observed on the ES+ series line cards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

Workaround: There is no workaround.

- CSCub42920

Symptoms: Keyserver rejects rekey ACK from GM with message (from **debug crypto gdoi ks rekey all**):

```
GDOI:KS REKEY:ERR:(get:0):Hash comparison for rekey ack failed.
```

The keys and policies in the rekey packet are correctly installed by the GM, but the rekey ACK does not get processed by the keyserver. This leads to rekey retransmissions, GM re-registration, and potential disruption of communication.

Conditions: Rekey ACK validation in versions Cisco IOS Release 15.2(4)M1 (Cisco ISR-G2) and Cisco IOS Release 15.2(4)S/Cisco IOS XE Release 3.7S (Cisco ASR 1000) is incompatible with other software releases.

A keyserver that runs Cisco IOS Release 15.2(4)M1 or Cisco IOS Release 15.2(4)S/Cisco IOS XE Release 3.7S will only be able to perform successful unicast rekeys with a GM that runs one of those two versions. Likewise, a keyserver that runs another version will only interoperate with a GM that also runs another version.

Workaround: Use multicast rekeys.

- CSCub46423

Symptoms: Connecting from Windows 7 L2TP/IPSec client to the VPN fails when using HSRP virtual IP as a gateway IP and Error 788 is displayed.

Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T or later releases, and the Windows 7 L2TP/IPsec VPN client.

Workaround: Downgrade to Cisco IOS Release 15.1(3)T.

- CSCub46570

Symptoms: The image cannot be built with an undefined symbol.

Conditions: This symptom occurs as the commit error triggers the compiling issue.

Workaround: There is no workaround.

- CSCub47520

Symptoms: “Match dscp default” matches router initiated ARP packets.

Conditions: This issue seen on Cisco 7600 ES+ line cards.

Workaround: Classify router generated packets using source mac address using a MAC ACL.

- CSCub48120

Symptoms: Sp crash is observed @oce_to_sw_obj_type on a router reload.

Conditions: This symptom is seen with core link flap at remote end during IP- FRR cutover.

Workaround: There is no workaround.

- CSCub49291

Symptoms: Static tunnels between hubs and spokes fail to rebuild.

Conditions: The symptom is observed when you reload the hub on the DMVPN IPv6 setup with DPD on-demand enabled on all spokes.

Workaround: There is no workaround.

- CSCub54872

Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

Workaround: Use a shorter prefix.

Further Problem Description: This issue does not affect software switching platforms.

- CSCub56064

Symptoms: Ping fails after doing EZVPN client connect if CEF is enabled.

Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

Workaround: There is no workaround.

- CSCub58312

Symptoms: When IGMP query with source IP address 0.0.0.0 is received on an interface, it is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  Internet address is 1.1.1.1/24
  IGMP querying router is 0.0.0.0 <-----
```

```
Router#sh ip igmp snooping mrouter
vlan          ports
-----+-----
```

```
1  Po1, Po8, Router<-----
```

Conditions: This symptom is seen when IGMP query with source IP address 0.0.0.0 is received.

Workaround: There is no workaround.

- CSCub58483

Symptom: The **radius-server attribute 6 on-for-login-auth** command is not configurable any more.

Conditions: There are no specific conditions under which this issue occurs.

Workaround: There is no workaround.

- CSCub59493

Symptoms: The CPU remains at 100% after the SNMPv 2c walk even after 5 minutes.

Conditions: This symptom occurs when an SNMP walk is done on mplsLsrStdMIB.

Workaround: There is no workaround.

- CSCub60678

Symptoms: Standby RSP is periodically reset after memory exhaustion. This can be checked by checking free memory on standby SP by the **show memory statistic**.

Conditions: This symptom is triggered by standby RSP restart or router reload.

Workaround: There is no workaround.

- CSCub62897

Symptoms: SVI is not coming up for a long time even there are active ports in that VLAN.

Conditions: This symptom is seen with flexlink with preemption and VLAN load balance configuration.

Workaround: There is no workaround.

- CSCub67101

Symptoms: The POS interface line protocol is down with encapsulation PPP in an MPLS setup.

Conditions: This symptom occurs when configuring encapsulation PPP on both ends of PE1 and CE1, and then configuring xconnect in the customer-facing interface of PE1.

Workaround: Reconfigure the xconnect settings. Then, the interface will come up in the proper state.

- CSCub73159

Symptoms: IOSD crash is seen.

Conditions: This symptom occurs when bringing up 8000 PPP sessions with QoS and eBGP routes.

Workaround: There is no workaround.

- CSCub73430

Symptoms: A Cisco router that is running the Cisco IOS Release 15.2(4)S ipbase9 feature set may crash.

Conditions: This symptom is seen when an interface with a QoS policy attached comes up.

Workaround: Use other feature sets, for example, adventerprise9.

- CSCub73787

Symptoms: A RSP720 may crash if a high rate of traffic is punted to the RP.

Conditions: This symptom is seen on a Cisco 7600 with RSP720. It is specific to a driver used only by the RSP720. Other supervisor models are not affected. The problem is only seen in Cisco IOS Release 15.1(3)S and later images, because of a code change made to the RSP720 driver.

Workaround: Isolate and stop the traffic being punted to RP.

- CSCub78830

Symptoms: Traffic matching WCCP service gets black-holed.

Conditions: This symptom is observed in vrf-wccp scenario and on redirection into MPLS cloud using GRE encap.

Workaround: There is no workaround.

- CSCub78917

Symptoms: PIM VRF neighbor is not coming up.

Conditions: This symptom is seen with MVPNv6 configurations.

Workaround: Use earlier images.

- CSCub79035

Symptoms: Multicast traffic will get route cached on the receiver/decap node resulting in traffic drop and slight increase in RP/SP CPU.

Conditions: This symptom is seen when multicast traffic flowing over GRE tunnel protected with IPsec and PIM is enabled on the GRE tunnel.

Workaround: There is no workaround.

- CSCub79102

Symptoms: Router crashes with MVPNv6 setup.

Conditions: This symptom is seen while unconfiguring VRF.

Workaround: There is no workaround.

- CSCub79590

Symptoms: The **match user-group** commands do not appear in the running configuration after being configured.

```
Configure an inspection type class-map:
class-map type inspect TEST
  match protocol tcp
  match user-group cisco
```

Save the configuration. Try to view the configuration in the running configuration:

```
hostname# show run class-map
building configuration...
```

```

Current configuration : 66 bytes
!
class-map type inspect match-all TEST
  match protocol tcp
end

```

But, view the configuration directly in the class-map:

```

hostname# show class-map type inspect
  Class Map type inspect match-all TEST (id 1)
    Match protocol tcp
    Match user-group cisco

```

The configuration never shows up in the running configuration, but it is in the class-map configuration. As a note, the functionality exists on the ZBFW, but the configuration does not show up in the running configuration.

Conditions: This symptom is only observed with the **match user-group** commands.

Workaround: This issue only affects devices after a reload as the router will read the startup configuration, which will not have the **match user-group** command. As a result, the **match user-group** commands need to be reentered after every reload.

- CSCub80491

Symptoms: A Cisco router may experience alignment errors. These alignment errors may then cause high CPU.

Conditions: This symptom occurs as the alignment errors require using Get VPN. It is currently believed to be related to having the Get VPN running on a multilink interface, but this is not yet confirmed.

Workaround: There is no workaround.

- CSCub90459

Symptoms: If CUBE has midcall reinvite consumption enabled, it also consumes SIP 4XX responses. This behavior can lead to dropped or hung calls.

Conditions: This symptom occurs when midcall reinvite consumption is enabled.

Workaround: There is no workaround.

- CSCub91428

Symptoms: Internal VLAN is not deleted even after waiting for 20 minutes, and the VLAN cannot be reused.

Conditions: This symptom is seen with any internal VLAN allocated dynamically that is not freed up after 20 minutes in the pending queue.

Workaround: There is no workaround.

- CSCub91546

Symptoms: Traffic is dropped silently on the VLAN.

Conditions: This symptom is observed when all the VLANs in the router are used (0 free VLAN). Any new internal VLAN creation will fail, and an appropriate error message is not shown.

Workaround: There is no workaround.

- CSCub91815

Symptoms: Certificate validation fails with a valid certificate.

Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

Workaround: There is no known workaround.

- CSCub93496

Symptoms: One-way video from CTS-1000 to TS-7010 is seen in the following topology:

```
CTS-1000 (v1.9.1) >>> CUCM 8.6.2aSU2 >>> CUCM 9.0 >>> CUBE 15.1.2T (2811) >>>
CUBE 15.1.4M4 (2951) >>> CUCM9.0 >>> VCS X7.1 >>> TS-7010 2.2
```

Conditions: This symptom occurs when SDP Passthru mode on CUBE is used.

Workaround: RTP payload types 96/97, which are associated with fax/faxack need to be remapped to some other unused values.

- CSCub94825

Symptoms: After Cisco IOS XE bootup, there are no static reverse routes inserted as a result of applying/installing and HA crypto map. The same issue is present on the HSRP standby device, namely, the static RRI routes will not get installed in case a failover occurs. The **show cry map** command can be used to verify that RRI is enabled. The **show cry route** command can be used to determine if RRI has happened and if it has been done correctly.

Conditions: This symptom is observed with the following conditions:

- Cisco IOS XE Release 3.5 up to Cisco IOS XE Release 3.7
- VRF-aware IPsec with stateless HA and static RRI - IPv4

Workaround: Removing and reentering the **reverse-route static** command into the configuration will actually trigger the route insertion.

- CSCub96743

Symptoms: A packet loss is seen with a stateful switchover (SSO) in a Cisco ASR 1000 router with scaled configuration.

Conditions: This symptom is a day one issue and is seen with a scaled configuration.

Workaround: There is no workaround.

- CSCub99756

Symptoms: The Cisco ASR 1000 router running Cisco IOS Release 15.2(4)S acting as a GM in a Get VPN deployment starts using the most recent IPsec SA upon KS rekey instead of using the old key up to 30 seconds of expiration.

Conditions: This symptom is observed only in Cisco IOS Release 15.2(4)S.

Workaround: There is no workaround.

- CSCuc06024

Symptoms: Traffic flowing through EVCs that do not belong to any service group will see incorrect bandwidth values because of wrong bandwidth value programmed on the port-default node.

Conditions: This symptom is seen when a mixture of flat and HQoS SGs having bandwidth configurations on their policies are applied on PC EVCs. Two mem- links are part of this PC, and default load-balancing is used.

Workaround: There is no workaround.

- CSCuc08061

Symptoms: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

Workaround: Reboot the spoke.

- CSCuc11853
Symptoms: T1 controller will stay DOWN after switchover.
Conditions: This symptom is seen when SATOP is configured on T1.
Workaround: Do a shut and no shut.
- CSCuc13364
Symptoms: Egress service policy on EFP is dropping all traffic in egress. Offered rate equals drop rate. Interface output rate is zero, and output drop is increasing.
Conditions: This symptom is observed with Cisco ME 36xx that is running Cisco IOS Release 15.2(2)S.
Workaround: There is no workaround.
- CSCuc14088
Symptoms: The default class is not being exported with the class option template.
Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.
Workaround: There is no workaround.
- CSCuc15203
Symptoms: If the ISM-VPN module is turned on and ZBFW is configured, when asymmetric routing occurs, the router crashes.
Conditions: This symptom occurs when the ISM-VPN module is turned on and ZBFW is configured, and when asymmetric routing occurs.
Workaround: There is no workaround.
- CSCuc15548
Symptoms: Subscriber session on LAC/LNS in attempting state with “vpdn authen- before-forward” CLI configured and auto-service in the RADIUS profile is getting stuck.
Conditions: This issue is seen with CLI “vpdn authen-before-forward” and one auto-service in the user profile in RADIUS.
Workaround: Configure and apply one policy-map with SESSION-START rule with at least one action.
- CSCuc15656
Symptoms: REP occasionally fails when a peer device that is running REP on the same segment is reloaded.
Conditions: This symptom is seen when a remote device is reloaded. The REP state machines on both devices can get stuck.
Workaround: Flap the link of the unit which did not go into the REP wait state. This will bring the REP state machines at both ends.
- CSCuc15695
Symptoms: The counters are not polling the correct stats.
Conditions: This symptom was first observed on the ATM interfere, but it is not particular to the ATM as this issue was reproduced on the Gigabit Ethernet interface as well.
Workaround: There is no workaround.

- CSCuc15810
Symptoms: MVPN over GRE PIM VRF neighbor is not up after SSO.
Conditions: This symptom is seen when MVPN over GRE PIM VRF neighbor is not up after SSO.
Workaround: There is no workaround.
- CSCuc19862
Symptoms: Traceback and CPU hog is seen due to spurious memory access when flexible NetFlow is enabled on the 4G cellular interface.
Conditions: This symptom is seen when enabling flexible NetFlow on 4G cellular interface.
Workaround: Use classic NetFlow or configure FNF on the tunnel template interface (preferred).
- CSCuc28757
Symptoms: IPv6 HbH Traffic traversing across BD SVIs will not be rate-limited by HbH rate-limiter that is configured.
Conditions: This symptom is seen when enabling HbH rate-limiter on an NP of ES+ and IPv6 HbH traffic traversing across SVIs part of EVC BD of ES+ interface.
Workaround: There is no workaround.
- CSCuc29310
Symptoms: TD probes in fast mode are gone when the link flaps (not PfR external interfaces).
Conditions: This symptom is observed with TD, fast mode, and link flap, which cause SAF session flap.
Workaround: Issue “clear pfr mas tr”.
- CSCuc29884
Symptoms: Outage and CPU remain astonishingly high against XDR MCAST process on a scaled HWO BFD testbed.
Conditions: This symptom is seen after a router reload, when OSPF converge is getting completed, and started 10g traffic through the box.
Workaround: There is no workaround.
- CSCuc41531
Symptoms: Forwarding loop is observed for some PfR-controlled traffic.
Conditions: This symptom is observed with the following conditions:
 - Traffic Classes (TCs) are controlled via PBR.
 - The parent route is withdrawn on selected BR/exit.Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).
- CSCuc44555
Symptoms: Multicast traffic is not forwarded to downstream, even when the groups show up in the group list.
Conditions: This issue is seen only when the traffic comes on RPF fail interface, and the downstream port is blocked due to STP or similar protocol.
Workaround: Disable IGMP snooping.

- CSCuc45115
Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at `nhrp_add_static_map`.
Conditions: This symptom is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.
Workaround: There is no known workaround.
- CSCuc45528
Symptoms: Incremental leaks are seen at `:_be_nhrp_rcv_error_indication`.
Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.
Workaround: There is no workaround.
- CSCuc46356
Symptoms: Router hangs and crashes by WDOG.
Conditions: This symptom occurs when IPv6 ACL is applied to a port-ch sub-if. The sub-if is deleted followed by deletion of the ACL.
Workaround: Delete the ACL before deleting the port-ch sub-if.
- CSCuc50482
Symptoms: With P2P GRE PIM enabled tunnels in Cisco 7600, high CPU might occur in standby SP. It could happen mostly when the tunnel is configured under a MVPN.
Conditions: This symptom may happen when running Cisco IOS Release 12.2(33) SRE7 and later releases.
Workaround: Boot up the standby with tunnel shut and then enable it once the standby is up.
- CSCuc52506
Symptoms: 6PE and 6VPE traffic drops are seen on shutting ECMP link.
Conditions: This symptom occurs after configuring the 6PE/6VPE between UPE-2 and UPE-1 with ECMP paths between both nodes. Shut the ECMP link to observe the traffic drop.
Workaround: There is no workaround.
- CSCuc64719
Symptoms: A Cisco ME 3600X HSRP failover is seen in VPLS.
Conditions: This symptom occurs when HSRP state changes from active to standby. The MAC address on the active router is not flushed.
Workaround: Clear MAC table on HSRP active router.
- CSCuc68743
Symptoms: A crash occurs while running CME smoke regression.
Conditions: This symptom is observed while running CME smoke regression.
Workaround: There is no workaround.
- CSCuc71706
Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

Workaround: There is no workaround.

- CSCuc97711

Symptoms: After SSO, traffic on P2P-GRE tunnel within a MVPN might be affected.

Conditions: This issue is seen in Cisco IOS Releases 12.2SREx and RLSx-based releases.

Workaround: **Shut/no shut** of P2P tunnel interface.