Caveats for Cisco IOS Release 15.1S

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (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 Caveats—Cisco IOS Release 15.1(1)S2, page 297
- Resolved Caveats—Cisco IOS Release 15.1(1)S1, page 307
- Open Caveats—Cisco IOS Release 15.1(1)S, page 335

Resolved Caveats—Cisco IOS Release 15.1(1)S2

Cisco IOS Release 15.1(1)S2 is a rebuild release for Cisco IOS Release 15.1(1)S. The caveats in this section are resolved in Cisco IOS Release 15.1(1)S2 but may be open in previous Cisco IOS releases.

- CSCsl18054

  Symptoms: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, not after failed logins.

  Symptoms: Occurs on a router running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCtg85402

  Symptoms: Multicast packet software switching MFIB platform flags “NP RETRY RECOVERY HW_ERR HAL” after SSO/ISSU.

  Conditions: Issue seen only with CFC cards and not with DFC. Specific to mVPN configuration with egress CFC cards. Issue seen under rare condition with SSO/ISSU.

  Workaround: Remove and add Default MDT configuration.

- CSCth84714

  Symptoms: With scaled number of MLP bundles on Sip200 with DLFI enabled, the sip200 crashes.

  Conditions: This symptom occurs with the following conditions: 1. Reload the SPA having MLP bundles. 2. Shut / No shut the controller. 3. Flap the links by any other means.

Workaround: The issue is not seen without high traffic and without LFI enabled.

- CSCti66454

  Symptoms: Router crashes when using the **show crypto session detail** command after using the **clear crypto session** command.

  Conditions: This symptom is observed when the router is running any form of tunnel protection, and SAs have been cleared. Then the user executes a **show** command.

  Workaround: Wait a few moments (30 seconds) between the **show** command and the **clear** command.

- CSCti81177

  Symptoms: Features like Videomon do not work on routed port.

  Conditions: This symptom occurs when an interface is configured as a switchport and reconfigured to routed Port.

  Workaround: Reload the line card.

- CSCti92812

  Symptoms: After physical interface flap, GRE tunnel for VRF does not come up correctly.

  Conditions: This symptom occurs when GRE tunnel is configured for default (global) routing table.

  Workaround: There is no workaround.

- CSCtj30238

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

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

  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtj56142

  Symptoms: ISG uses dummy user-name within EAP re-authentication related access-requests as the session identifier.

  Conditions: The symptom is observed during EAP re-authentications and likely after CoA-based service activation on an EAP-authenticated session. This happens only when the EAP access-requests carry a dummy user-name and access- accept does not have the correct username.

  Workaround: There is no workaround.

- CSCtj58405

  Symptoms: Full multicast traffic is not sent from the source PE.

  Conditions: The issue is observed only with ECMP links and with a higher scale (above 75 MVRF and 100 mroutes per VRF) for default MDTS. It is seen when one of the ECMP links which was down earlier, comes up. If all the ECMP links are already up, then the issue is not seen.

  Workaround: Clear the IP mroute using **clear ip mroute** command.

- CSCtj61748

  Symptom: Service activation fails occasionally.

  Conditions: This symptom occurs with multiple services in the session authentication or authorization response that are configured in the same service-group.

  Workaround: Remove fields that are related to “service-group” or “service- type” in service definitions.

- CSCtj79769

  Symptoms: LC crashes.

  Conditions: When disabling MLD snooping on an interface or disabling IPV6 multicast in general.

  Workaround: There is no workaround.

- CSCtj85333

  Symptoms: System may crash when config-template contains the config commands “ip ips signature-category” and when the template is downloaded to the router using the CNS config feature commands “cns config retrieve” exec command, “cns config initial” config command. This symptom may also occur when the config template is downloaded to the router using the device Config-Update operation of Config Engine.

  Conditions: This is normal mode operation, but this symptom will occur when such CNS feature is used.

  Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do Shut/no shut on PfR master or PfR border.

- CSCtj91764

  Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

  Conditions: The crash happens during a complete SNMP MIB walk.

  Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 SA dual per session, a crash happens on Crypto_SS_process.

  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and four SA dual per session.

  Workaround: There is no workaround.

- CSCtj99431

  Symptoms: Session have shared key mismatch between ISG and Radius client. Non- subnet client (Best Match) does get preference over subnet client.

  Conditions: This symptom is observed on a Cisco ASR1000 series router when it functions as an ISG Radius-Proxy router.

  Workaround: Remove “ignore server key” from “aaa server radius dynamic-author”.

- CSCtk18607

  Symptoms: Router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Conditions: This symptom occurs at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

  Workaround: There is no workaround.

- CSCtk32104

  Symptoms: PPPoE data traffic gets process switched.

  Conditions: This symptom occurs on PPPoE data traffic.

  Workaround: There is no workaround.

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: This symptom is observed only if DUT has an eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from the VPNv4 peer.

  Workaround: A hard reset of the session will remove the dampening information.

- CSCtk36582

  Symptoms: Accounting on/off messages from AZR clears session from all the sessions in the client pool.

  Conditions: This symptom occurs in the following scenarios: 1) When there are two AZRs, 192.168.100.1 and 192.168.100.2, and you configure the client in the ISG under radius proxy as “client 192.168.0.0 255.255.0.0”. 2) Accounting on or off from any of the clients is clearing sessions from both the clients.

  Workaround: Configure clients individually instead of pool configuration.

- CSCtk53657

  Symptoms: WCCP black-holes traffic, if WCCP is disabled on the cache engine.

  Conditions: This symptom occurs when you configure WCCP to use L2 / Mask on the cache engine, leave the router interface up with the cable connected and disable WCCP on the cache engine. When the “SERVICELOST” message appears on the Cisco 7600 and the hardware is still programmed, WCCP blackholes the traffic.

  Workaround: There is no workaround.

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while performing “write memory” or “show running configuration” on the router after configuring “privilege exec level 15 show adjacency”.

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62950

  Symptom: SSH over IPv6 may crash the router.

Conditions: This symptom occurs with SSH over IPv6.

Workaround: There is no workaround.

- CSCtk66080

  Symptoms: LACP/PAGP BPDUs are not tunneled by EVC Xconnect on ES+ and ES20.

  Conditions: This symptom occurs with EVC Xconnect with encapsulation untagged/deault and LACP/PAGP BPDUs ingressing on it.

  Workaround: There is no workaround.

- CSCtk67455

  Symptoms: The fragmented traffic is dropped when the LOG option is set for IPv6 ACLs on 3CXL PFC-based supervisors.

  Conditions: This symptom is observed when the LOG keyword is specified for IPv6 ACLs on 3CXL PFC mode.

  Workaround: There is no workaround.

- CSCtk67768

  Symptoms: RP crash is observed in DHCPD receive process.

  Conditions: This symptom occurs on Cisco IOS DHCP server that is used on Cisco IOS ASR routers and acting as ISG.

  Workaround: There is no workaround.

- CSCtk68109

  Symptoms: A Cisco ASR 1000 router reloads when running CVP survivability TCL.

  Conditions: This symptom is observed when “pass-thru content sdp” is used in the Cisco ASR 1000 router configuration.

  Workaround: Use “codec transparent” instead of “pass-thru content sdp”.

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

  Workaround: There is no workaround.

- CSCtk95106

  Symptoms: CPU 1 of SPA 8XT1E1 goes into a forced reload followed by a software forced reload of line card SIP-200 when a multilink PPP with interleave enabled having fragment size 42 is disabled and enabled. One member of the link is removed.

  Conditions: This issue is noticed when traffic is pumped onto the DUT from remote end. Size could be as low as 800 bytes. Interleave is disabled and enabled on the mulilink interface, and one of the members of the MP is detached from the bundle using the **no ppp multlink group** <> command.

  Workaround: There is no workaround.

- CSCtk95742

  Symptoms: Traffic does not flow from EVC-BD.

  Conditions: This symptom occurs with port-channel EVC-BD configuration with ES20 memberlinks. This symptom occurs if ES20 LC is replaced with the ES+ LC and added the same port as ES20 to the port-channel.

Workaround: Remove and add the EVC.

- CSCtl00127

  Symptoms: The output of **show ip int** command does not indicate whether the "ip security ignore-cipso" option is configured and/or operational.

  Conditions: Configure "ip security ignore-cipso" on an interface. This was not indicated on the **show ip interface** *interface name* command output of that interface.

  This symptom is observed on the following devices:

  - Cisco IOS Catalyst 6500 router that is running Cisco IOS Releases 12.2(33)SXH and 12.2(33)SXI.
  - Cisco IOS Catalyst 7600 router that is running Cisco IOS Releases 12.2(33)SRA7, 12.2(33)SRB, 12.2(33)SRC, 12.2(33)SRD, and 12.2(33)SRE.
  - Cisco IOS Catalyst 4500 router that is running Cisco IOS Release 12.2(40)SG.

  The output is indicated correctly when it is enabled on Cisco IOS Release 12.2(18)SXF17a.

  Workaround: There is no workaround.

- CSCtl05785

  Symptoms: Connectivity is broken on Cisco 7600 L3 subinterfaces upon reconfiguration of the assigned VRF. Directly connected devices are no longer reachable. Input path is broken (packets are seen in netdr but do not reach the RP).

  Conditions: This symptom is observed on Cisco 7600 routers that are running Cisco IOS Release 12.2(33)SRE2. This issue is seen on Sip-400 subinterfaces.

  Workaround: Reload the router.

- CSCtn07415

  Symptoms: Crash is observed at crypto_map_get_map_method_bitmask while reconfiguring IPSec with 1300 GRE tunnel interfaces, with old configurations still present.

  Conditions: This symptom occurs with IPSec with GRE tunnel interfaces.

  Workaround: There is no workaround.

- CSCtl07955

  Symptoms: BFD neighbor goes down and does not come up again when an unrelated LC is powered down by using the **no power enable module X** command.

  Conditions: This symptom occurs when an unrelated LC is powered down.

  Workaround: There is no workaround.

- CSCtl22871

  Symptoms: CoS value (applied from setcos policy) does not get copied to EXP while adding a label to the VPLS case, VPLS cfgd on EVC BD Vlan.

  Conditions: This symptom occurs on ES+ and QoS policy-map when set CoS is applied on EVC BD with VPLS configured on BD Vlan.

  Workaround: There is no workaround.

- CSCtl71478

  Symptoms: In an HA system, the following error message is displayed on the standby RP and LC: "OCE-DFC4-3-GENERAL: MPLS lookup unexpected".

Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

Workaround: There is no workaround.

- CSCtl79512

  Symptoms: The default BRR of the L2 node is configured as 255.

  Conditions: This symptom is observed when applying port-shaper on port channel main interface. Configure EVCs on port channel with two EVCs having HQoS policy-map and with two other EVCs having service-group with HQoS policy- map.

  Workaround: There is no workaround.

- CSCtl90890

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic and in some cases may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn15877

  Symptoms: For access subinterface, ingress stats on the **show interface** *interface type number* **stats** command will not work.

  Conditions: The issue is seen only on access subinterface.

  Workaround: There is no workaround.

- CSCtn16840

  Symptoms: VPLS imposition traffic does not go through for some of the VCs when the core is a port channel on ES20.

  Conditions: This symptom is observed when core facing is a port channel on ES20.

  Workaround: Do a shut/no shut on the port channel.

- CSCtn16899

  Symptoms: PIM neighborship is lost between source node and receiver nodes.

Conditions: This issue is seen when TE FRR is configured for the link between source node and root node and after FRR cutover is done.

Workaround: Shut and no shut the egress interface of the backup tunnel on the root node.

- CSCtn17267

  Symptoms: Broadband call admission control (CAC) is not working.

  Conditions: This symptom occurs under the following conditions:

  1. DHCP initiated sessions.
  2. PPPoE sessions on an interface where IP session configurations are present.

  Workaround: There is no workaround.

- CSCtn17680

  Symptoms: When performing an OIR on a Cisco WS-X6708 module, the router may crash. When inserting the card, the following message is displayed:

  ```
  %EARL_L2_ASIC-SP-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr. Error occurred. Ctrl1
  0xB88D0E3D
  ```

  Then, the following message is displayed:

  ```
  %CPU_MONITOR-SP-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 60 seconds
  [*Sched* 41%/0% (00:01:00.244 99%/99%)]
  ```

  Finally, a timeout occurs, followed by the crash:

  ```
  %CPU_MONITOR-SP-3-TIMED_OUT: CPU_MONITOR messages have failed, resetting system
  (self) [5/0]
  ```

  Conditions: This symptom is observed on Cisco IOS 7600 series routers with either a single or dual RSP720 supervisor. In the case of dual supervisors, both supervisors crash. The cause of the crash is unknown. However, after the router reloads, the affected module has been installed again without further issue in a couple of instances.

  Workaround: There is no workaround.

- CSCtn19444

  Symptoms: mLACP memberlinks may be bundled on an isolated PoA with a core failure, resulting in both PoAs becoming active.

  Conditions: This symptom occurs when running mLACP. The ICRM connection between the PoAs is lost. The PoAs are in a split brain situation and both PoAs attempt to become active. If the interface configured as “backbone interface” goes down on one of the PoAs, that PoA may keep the port-channel memberlinks bundled. The end result is that both PoAs are in mLACP active state, and both have their port-channel memberlinks bundled. After the fix the PoA with the backbone interface failure will unbundle its port-channel memberlinks, leaving only one PoA as active.

  Workaround: Configure shared control by configuring “lacp max-bundle” on the Dual Homed Device (DHD) if the device supports it. This would prevent the DHD from bundling the memberlinks to both PoAs at the same time.

- CSCtn22728

  Symptoms: See the following:

  Router(config)#monitor session 1 type erspan-source

  Router(config-mon-erspan-src)#destination ?

  <cr>

  Router(config-mon-erspan-src)#destination int g11/48

Router(config-if)#

Config Sync: Line-by-Line sync verifying failure on command:

destination int g11/48

due to parser return error

Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

Workaround: Do not issue not applicable commands.

- CSCtn24024

  Symptoms: A Cisco ASR 1000 router with dynamic crypto maps may intermittently experience a condition where an IPSec SA will decrypt traffic but not encrypt traffic.

  This is generally seen when the remote peer IP address has changed.

  It is observed that there is a duplicate flow created in the hardware and therefore the traffic to be encrypted matches a stale flow so that packets are not encrypted to the right peer.

  Conditions: This symptom is observed when dynamic crypto maps are used.

  Workaround: Try to clear the crypto session from the spoke. In some cases when the new IPSec SA is built, it will correct the problem.

- CSCtn38711

  Symptoms: A router crashes.

  Conditions: This symptom occurs during SSO on a heavily loaded Cisco 7600 router.

  Workaround: There is no workaround.

- CSCtn41245

  Symptoms: Subinterface ingress stats do not work for access subinterfaces.

  Conditions: This symptom is observed only for the access subinterface. Interface stats and regular subinterface stats work as expected.

  Workaround: There is no workaround.

- CSCtn41662

  Symptoms: Standby RP crashes sometimes when policymap configuration is done. This crash happens randomly with the following crash decode:

  ```
  0xA65C01C:qm_make_final_vmr(0xa65bf14)+0x108
  0xA64799C:qm_send_merge_replace_request(0xa647834)+0x168
  0xA6471B0:qm_tm_merge_replace(0xa646ee4)+0x2cc
  0xA63B3FC:qm_tcam_modify_service_policy(0xa63adbc)+0x640
  0xA63A8AC:qm_process_mqc_event_hdlr(0xa63a51c)+0x390
  0xA63BE7C:qm_process_events_q_hdlr(0xa63bad0)+0x3ac
  0xA63CAA0:qm_process(0xa63c9cc)+0xd4
  ```

  Conditions: This symptom occurs randomly when policymap, class-map is modified, which is applied on different interfaces. This does not happen consistently.

  Workaround: There is no workaround.

- CSCtn45777

  Symptoms: Align messages are seen when enabling the **debug cwan atom** debug command.

  Conditions: This symptom is observed when the **cwan atom** debug command is enabled. Spurious memory access messages are seen on the router console.

Workaround: There is no workaround.

- CSCtn64500

  Symptoms: Multicast traffic does not pass through an ATM point to a multipoint subinterface.

  Conditions: This issue is caused by an incomplete inject p2mp multicast adjacency on ATM P2MP interface. The output of the **show adjacency ATM interface detail** command shows that the Inject P2MP multicast adjacency is in incomplete state.

  Workaround: Run the **clear adjacency** command to force repopulating the incomplete adjacency. Note that you should be aware of the impact of this system-wide command. As an alternative, use unicast commutation if it is possible to do so.

- CSCtn68329

  Symptoms: When source and receivers are in the same VLAN, receivers are unable to receive multicast traffic unless IGMP snooping is disabled for the VLAN.

  Conditions: This issue is not seen when VLAN is in global routing table (no MVPN).

  Workaround: Disable IGMP snooping for the VLAN.

- CSCtn89179

  Symptoms: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA

  Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later releases

  Workaround:

  1. Apply a service policy similar to below:

     ```
     policy-map test1
     class class-default
     queue-limit 496 --> (this number is a interface bandwidth(in kbps)*1000 / (8
     * 250 * 2) value for the correct behavior.)
     ```

  2. Or reload of the LC.

- CSCtn95395

  Symptoms: VTEMPLATE Background Mgr crashes on DVTI server after using the **clear crypto session** command on DVTI client.

  Conditions: This symptom is seen on DVTI server when sessions are setting up with the IPSec DVTI configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. We might run into VTEMPLATE Background Mgr process crashing after executing the **clear crypto session** command a couple of times on DVTI client.

  Workaround: There is no workaround.

- CSCtn98521

  Symptoms: After the CLI is enabled on ES+ for the control packets hitting on ES+ to not go into special queue, CLI does not reflect in the running configuration on RP sometimes.

  Conditions: This symptom occurs after enabling the **platform control- packet use-priority-q disable** command on ES+ for the control packets hitting on ES+ to not go into special queue. CLI does not reflect in the running configuration on RP.

  Workaround: There is no workaround.

- CSCtn98562

  Symptoms: CLI is enabled on ES+ for the control packets hitting on ES+ to not go into special queue. When doing ES40 LC OIR, control packets that are seen hitting on ES+ port are bypassing the QoS that is configured on the port, and all packets are going in hi-p interface queue.

  Conditions: This symptom is observed after enabling the **platform control-packet use-priority-q disable** command on ES40 LC OIR. The control packets that are hitting on ES+ port are bypassing the QoS that is configured on the port, and all packets are going in hi-p interface queue.

  Workaround: There is no workaround.

- CSCtn99440

  Symptoms: LC CPU high is due to the mfib-const-lc process.

  Conditions: This symptom is observed for scaled mvpn gre configs when more gre mdt tunnels come up.

  Workaround: There is no workaround.

- CSCto08790

  Symptoms: When BRAS is applying an ANCP shaper with specific policy-map name, ActualDownstreamRate and dslType value, a policy-map is created with a policy-map name resulting in hash value 0.

  Policy-map names with Hash value 0 are not handled properly by QoS client and cause the router to crash.

  Conditions: This symptom is seen with certain policy-map or class-map names that can result in internal hash algorithm generating hash value 0, and therefore invalid policy-map or class-map id causes IOSD to crash.

  Workaround: There is no workaround.

- CSCto44585

  Symptoms: Packets with DF-bit set across the l2tpv3 tunnel are punted/dropped on the CPU.

  Conditions: This symptom occurs when PMTU in pseudowire-class configuration is enabled.

  Workaround: Reduce MTU on client side.

- CSCto61263

  Symptoms: With port-channel service-instance (EVC), the traffic stops flowing on new member-links added across different NP on ES+.

  Conditions: This symptom is seen with Cisco 7600, ES+ line card, port-channel service-instances (EVC) with member-links on different NP on a line card.

  Workaround: Use the **shutdown** command followed by the **no shutdown** command on the port channel main interface to resolve the issue.

Resolved Caveats—Cisco IOS Release 15.1(1)S1

Cisco IOS Release 15.1(1)S1 is a rebuild release for Cisco IOS Release 15.1(1)S. The caveats in this section are resolved in Cisco IOS Release 15.1(1)S1 but may be open in previous Cisco IOS releases.

- CSCta43825

  Symptoms: A CMTS walk of the ARP table causes high CPU usage. This symptom is also seen with an SNMP walk of the ARP table.

Conditions: This symptom is observed in the Cisco IOS 12.2S train.

Workaround: To prevent high CPU usage due to SNMP walk, implement SNMP view to prevent SNMP walk of the ARP table:

```
snmp-server view cutdown iso included
snmp-server view cutdown at excluded
snmp-server view cutdown ip.21 excluded
snmp-server community public view cutdown ro
snmp-server community private view cutdown rw
```

Further Problem Description: This symptom is widely observed in Cisco IOS 12.2S train since the ARP redesign in 2004. It is not an efficient way to do next search/tree walk. When there are a lot of ARP entries, the CPU utilization can reach as high as 99% when polling ipNetToMediaTable or atTable (they share the same logic).

- CSCtc73759

  Summary: The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml

- CSCtd10712

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtd16959

  Symptoms: Traceback is seen on SSO switchover.

  Conditions: This symptom is observed under the following conditions:

  - Configure CBTS master tunnel with 3 member tunnels
  - Delete all 3 member tunnels and then remove master command from master tunnel so it becomes regular TE tunnel
  - Configure auto-tunnel primary and backup setup
  - Make SSO switchover

  Many different tracebacks are seen on newly active RP, which are related to MPLS TE.

  Workaround: Do not delete CBTS Tunnels.

- CSCtd72318

  Symptoms: Cisco ASR 1004 router crashes at in __be_dhcpc_for_us.

Conditions: This symptom occurs when running Cisco IOS Release 12.2(33)XNC2. This is possibly associated with DHCP configuration.

Workaround: There is no workaround.

- CSCtd78587

  Symptoms: A Cisco Catalyst 6000 switch running Cisco IOS Release 12.2SX software might crash under rare conditions when err-disable recovery tries to recover a port. The following messages are seen in the logs before the switch resets itself:

  ```
  %CPU_MONITOR-6-NOT_HEARD
  ```

  Conditions: This symptom may be observed after the following sequence of events:

  3. An interface on the switch gets err-disabled as expected due to a certain feature; for example, due to BPDU Guard
  4. Shortly after, before BPDU Guard err-disable recovery kicks in, the same port gets err-disabled for a different reason; for example, because a diagnostic error is detected on the already err-disabled port
  5. Err-disable recovery (BPDU Guard) tries to recover the port and this leads to the crash.

  Workaround: Disable err-disable recovery.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCte15193

  Symptoms: The **no spanning-tree vlan [vlanno]** command is not removed on standby alone.

  Conditions: The symptom is observed under the following conditions:

  – the **no spanning-tree vlan** *vlanno* command is configured first
  – the **default spanning-tree vlan** *vlan- range* command is entered next
  – the vlanno falls within the designated range, but the last vlan number in the range does not have “no spanning-tree vlan <>”configured for that.

  Workaround: Enter the **default spanning-tree vlan** *vlanno* command to remove it.

- CSCte56437

  Symptoms: NAT programming on a Cisco Catalyst 6500 may become corrupted; the source and/or destination IP addresses of traffic passing through the NAT box are changed to the wrong IP addresses.

  Conditions: This symptom is observed when the NAT configuration is changed during a high-volume traffic session.

  Workaround: There is no workaround.

- CSCte65688

  Symptoms: Easy VPN server prints “Client_type=UNKNOWN” in “%CRYPTO-6-EZVPN_CONNECTION_UP: (Server)” log, when Software VPN Client establishes an IPSec session.

  Conditions: The symptom is observed when:

  – Easy VPN is configured between a Cisco VPN Client and an IOS router.

– "crypto logging ezvpn" is configured.

Workaround: There is no workaround.

Further Problem Description: This is simply a cosmetic issue. Currently, this message can identify hardware VPN clients (IOS/PIX/VPN3002) only.

- CSCtf23298

  Symptoms: There is high CPU usage when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Conditions: This symptom occurs when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Workaround: Remove single connection option.

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash upon doing a shut/no-shut on the tunnel interface of the other hub.

  Conditions: The symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.
  2. Hub 2 tunnel is shut and unshut.
  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: The symptom is observed with the following setup and configuration:

```
Router 1:
interface e0/0
ip address 192.168.1.1 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.10.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.2
ip route  10.20.0.0 255.255.0.0 e0/0 192.168.1.2

Router 2:
interface e0/0
ip address 192.168.1.2 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.20.1.1 255.255.0.0
exit

ip route static bfd e0/0 192.168.1.1
ip route  10.10.0.0 255.255.0.0 e0/0 192.168.1.1

interface e0/0
```

```
no ip route static bfd e0/0 192.168.1.1
```

Though the BFD state is DOWN the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtg18555

  Symptoms: A memory leak is observed with process_online_diag_pak.

  Conditions: This symptom is observed on a card supporting TestNonDisruptiveLoopback and TestFabricChHealth tests.

  Workaround: Disable the HM tests TestNonDisruptiveLoopback and TestFabricChHealth on LCs to stop the leak.

- CSCtg28806

  Symptoms: Router crashes at PKI manual enroll.

  Conditions: The symptom is observed on a Cisco 2921 router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link, it is mistakenly marked as “parallel p2p adjacency suppressed”.

  Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCth02812

  Symptoms: A prolonged unicast flood can be seen on an ingress path after a TCN event. The flood will last until entries in the arp table are refreshed.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SXH3a (issue has been tracked back to Cisco IOS Release 12.2(18)SXF in an L2 asymmetric environment. The flood is only seen if there is no bi-directional flow on the switch. This issue can be seen in all STP modes.

  Workaround: Clearing ip arp will correct this issue. Lowering the arp timeout will also minimize the impact of the flood.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCth13415

  Symptoms: One way audio in call transfer due to 491 response during resume re- INV.

Conditions: The symptom is observed when you have an UPDATE message passing through the CUBE and then a re-INV crossover happens. The re-INV crossover results in a 491 but the 491 is not correctly forwarded by the IPIP GW. This can result in one way audio issues if the crossed over re-INV was changing the media state from hold to resume.

Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening”.

  Conditions: The symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4.
  - eBGP + VPNv4 peer session is established and DUT.
  - Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth60232

  Symptoms: The port-channel interface may flap when adding or removing a VLAN from the trunk on a port-channel interface when one or more interfaces are in a state other than P or D.

  Conditions: This symptom is observed only when the port-channel interface has interfaces in states other than P or D.

  Workaround: Shut down the non-P members and make the vlan changes.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate video stream.

  Conditions: There are a couple of scenarios where this problem was observed.

  Scenario 1: This problem was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

  7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server

  1. Call is originated by 7985
  2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response

     m=video 53722 RTP/AVP 96 97 34 31
     b=AS:1920
     a=rtpmap:96 H264/90000
     a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600
     a=rtpmap:97 H263-1998/90000
     a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1
     a=rtpmap:34 H263/90000
     a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1
     a=rtpmap:31 H261/90000
     a=fmtp:31 CIF=1;QCIF=1
     a=sendrecv
  3. CUBE sets video m-line to 0 in the SDP of the SIP “ACK” response

     m=video 0 RTP/AVP 96

  Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

Workaround: There is no workaround.

- CSCth69364

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

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

- CSCth82164

  Symptoms: When OCSP is being used as the revocation check method for IKE, only the 1st connection attempt (after reboot or cache clearing of public RSA keys) undergoes an OCSP check. Subsequent revocation checks are bypassed because the peer's public key appears to be cached indefinitely.

  No CRL or other lifetime parameters are involved, OCSP should be consulted for each IKE tunnel setup.

  The following messages indicate bypassing the revocation check:

  ```
  ISAKMP:(1002): peer&apos;s pubkey is cached
  CRYPTO_PKI: Found public key in hash table. Bypassing certificate validation
  ```

  Conditions: This symptom is occurs when OCSP is configured as revocation check method for IKE.

  Workaround: There is no workaround.

- CSCth93218

  Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCti08811

  Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti25319

  Symptoms: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute Open Shortest Path First (OSPF) is configured.

  Conditions: This symptom occurs only for those configurations in which a network mask covers multiple supernets. For example, for the following network statement, router ospf 1 network 192.168.0.0 0.255.255.255 area 0 the above mentioned symptom occurs if the interfaces are configured with IP addresses as follows:

```
ip address 192.168.0.1 255.255.255.0
    ip address 192.168.1.1 255.255.255.0
    and so on.
```

  Workaround 1: Enable OSPF using interface command “ip ospf <AS> area”.

  Workaround 2: Configure multiple network statements with mask/wildcard equal to supernet as shown in the example below:

```
router ospf 1
    network 192.168.0.0 0.0.0.255 area 0
    network 192.168.1.0 0.0.0.255 area 0
    and so on.
```

- CSCti25339

  Symptoms: Cisco IOS device may experience a device reload.

  Conditions This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  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-2010-3050 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

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when “next-hop-unchanged allpaths” is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
 set ip next-hop <router ip address>
!
router bgp <asn>
 address-family ipv4 vrf <vrf name>
 redistribute static route-map static-nexthop-rewrite
 exit-address-family
 exit
exit
```

Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

For example, if you had:

ip route x.x.x.x 255.255.255.0 y.y.y.y

And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

ip route x.x.x.x 255.255.255.0 interface serial2/0

Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration "set ip next-hop self" is added to route-maps.

When used in conjunction with the newly added configuration:

```
router bgp <asn>
 address-family vpnv4 unicast
  bgp route-map priority
```

The "set ip next-hop self" will override "next-hop unchanged allpaths" for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34462

  Symptoms: After FPD upgrade, a **shut** on the active shows **no shut** on the standby.

  Conditions: The symptom is observed after an FPD upgrade.

  Workaround: Perform a **no shut** then shut the interface on the active to sync it properly.

- CSCti36310

  Symptom: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attributes are pulled by SNMP.

  Conditions: This symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

  Workaround: There is no workaround.

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

- The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword “established” or “eq bgp”.
- It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
- When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
- Both peers must be multisession capable.
- “transport multi-session” must not be configured on either device, or enabled by default on either device.
- “graceful restart” must not be configured.

Workarounds:

1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor.
3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where “neighbor x.x.x.x transport single-session” is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, and the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the Cisco IOS Release 12.2(33)SB router is the one not reloading.

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti61949

  Symptoms: Unexpected reload with a “SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and “chunk name is BGP (3) update” messages.

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67429

  Symptoms: A REP segment configured on 7600-ES+20G3CXL interfaces on a Cisco 7600 series router that is running Cisco IOS Release 15.0(1)S is not recovering as expected upon link failure recovery of the edge port configured on the 7600. A traffic storm triggered by ISIS protocol configured between 7600 and the MWR 2941s in the REP ring is occurring when the failed REP edge port becomes operational again.

  Conditions: The symptom is observed with a REP ring including two Cisco 7600 series routers equipped 7600-ES+20G3CXL and running Cisco IOS Release 15.0(1) S configured with ISIS and MPLS LDP. The problem is also present in Cisco IOS Release 12.2(33)SRE1.

  Workaround: Configure static routes between the 7600 routers and the MWR 2941s instead of ISIS.

- CSCti68721

  Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti74962

  Symptoms: "%PM-SP-4-PORT_BOUNCED: bounced by Consistency Check IDBS UP" message is seen on A3-1 new active router after line card OIR followed by an SSO switchover.

  Conditions: This symptom will occur only with a line card OIR followed by an SSO switchover.

  Workaround: There is no workaround.

- CSCti84762

  None

  update generation is stuck with some peers held in refresh started state(SE).The workaround is only hard reset of the stuck peers

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword.
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
  3. Change the configuration in such a way that nexthop is reachable.
  4. Configure a new static route through the same nexthop IP address used in step 1.

Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti94938

  Symptoms: With more than 1 L2TP sessions on virtual template interface, when applying non-existent route-map and modifying non-existent route map, router crashes.

  Conditions: This symptom occurs with PPPoE sessions with modifying policy configuration with non-existent route-map.

  Workaround: Configure route-map first before applying policy.

- CSCti97759

  Symptoms: IPSG configuration with DHCP snooping entry configuration causes the RP to crash.

  Conditions: This is seen when DHCP static entry is configured.

  Workaround: There is no workaround.

- CSCti98931

  Symptoms: Some sessions may be lost after Layer 2 Tunneling Protocol (L2TP) switchover.

  Conditions: This symptom occurs after L2TP switchover.

  Workaround: There is no workaround.

- CSCtj05591

  Symptoms: Memory corruption and SP crash seen.

  Conditions: The symptom is observed when creating 600 subinterfaces as OIF for Mroute entries.

  Workaround: There is no workaround.

- CSCtj08533

  Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

  Conditions: The symptom is observed when there are redundant paths to the CPE.

  Workaround: Use only one path between PE and CPE.

- CSCtj17316

  Symptoms: EIGRP flaps up and down in a large scale network, when there is a lot of data to be sent.

  Conditions: In an EIGRP network that has a large number of peers on a single interface, EIGRP might stop sending data to peers. This causes a flap due to packets not being acknowledged.

  Workaround 1: Find the instability in the network and fix the interface.

  Workaround 2: Summarize more routes.

  Workaround 3: Change more routers to stub.

  Workaround 4: Upgrade to rel7 of EIGRP.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

```
template peer-session ce-v4
  transport connection-mode passive
```

- CSCtj17667

  Symptoms: The **debug radius** debug command may cause memory corruption and crash in rp2 and 1ru images.

  Conditions: This symptom is seen with the **debug radius** command in rp2 and 1ru images.

  Workaround: Do not use the **debug radius** command.

- CSCtj20362

  Symptoms: Router does not allow configuring more than one secondary IP address in the same subnet, on an interface in the same VRF.

  Conditions: This symptom occurs when configuring a secondary address on an interface, which has already one secondary IP address in the same subnet. This applies to VNET capable interfaces.

  Workaround: There is no workaround.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different, the problem does not happen):

  Router1#sho inv

  NAME: “chassis”, DESCR: “2801 chassis” PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF

  NAME: “motherboard”, DESCR: “C2801 Motherboard with 2 Fast Ethernet” PID: CISCO2801 , VID: V04 , SN: FOC11456KMY

  NAME: “VIC 0”, DESCR: “2nd generation two port EM voice interface daughtercard” PID: VIC2-2E/M= , VID: V , SN: FOC081724XB

  NAME: “WIC/VIC/HWIC 1”, DESCR: “4 Port FE Switch” PID: HWIC-4ESW , VID: V01 , SN: FOC11223LMB

  NAME: “WIC/VIC/HWIC 3”, DESCR: “WAN Interface Card - DSU 56K 4 wire” PID: WIC-1DSU-56K4= , VID: 1.0, SN: 33187011

  NAME: “PVDM 1”, DESCR: “PVDMII DSP SIMM with one DSP with half channel capcity” PID: PVDM2-8 , VID: NA , SN: FOC09123CTB

  Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is done:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
  chunkmagic 120000 chunk_freemagic 4B310CC0
  -Process= "BGP Scanner", ipl= 0, pid= 549 with call stack
  0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
  0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
  0x403A4E84:bgp_scanner(0x403a4c50)+0x234
  ```

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

  ```
  Router# show ip bgp sum
  BGP router identifier 10.0.0.1, local AS number 65000
  BGP table version is 1228001, main routing table version 1228001 604000
  network entries using 106304000 bytes of memory
  604000 path entries using 31408000 bytes of memory
  762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
  ```

```
381 BGP AS-PATH entries using 9144 bytes of memory
382 BGP community entries using 9168 bytes of memory
142685 BGP route-map cache entries using 4565920 bytes of memory
```

The **clear ip bgp *** command is not a very common operation in production network.

Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an “Exit Mismatch” message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

  Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

  Workaround: There is no workaround.

- CSCtj30155

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

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

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1
    redistribute connected
    no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj32769

  Symptoms: Data path fails with Layer-2 Virtual Private Network (L2VPN)on ACR interface when asynchronous mode is enabled.

  Conditions: This issue occurs when a VPN is configured on ACR interface in asynchronous mode with cellpacking configurations. This issue does not occur in normal synchronous mode or Layer-2 Virtual Circuits (L2VCs).

  Workaround: Configure the same Maximum Number of Cells Packed (MNCP) value for local and remote provide edge (PE) devices.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38606

  Symptoms: The following error message is seen:

  ```
  %SYSTEM_CONTROLLER-3-MISTRAL_RESET: System Controller is reset:Normal Operation
  continues
  ```

  The **show ibc** exec command reports increments of the following counter:

  Hazard Illegal packet length = 7580

  Conditions: The symptom is observed on a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCtj40564

  Symptoms: Cisco ASR 1000 router disallows incoming Internet Key Exchange (IKE) connection that matches a keyring. This issue occurs after the router is reloaded.

  Conditions: This symptom occurs when a crypto keyring, which has a local- address defined as an interface, is used.

  ```
  crypto keyring keyring_test
    pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
    local address Loopback2104
  ```

  Workaround: Use an IP address.

  ```
  crypto keyring keyring_test
    pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
    local address <ip address>
  ```

- CSCtj46297

  Symptoms: Ping fails when performing a shut/no shut on the outgoing interface in an FRR setup.

  Conditions: The symptom is observed in an FRR setup when performing a shut/no shut on the outgoing interface.

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

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

  Workaround: There is no workaround.

- CSCtj48629

  Symptoms: Though “ppp multilink load-threshold 3 either” is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj50072

  Symptoms: High CPU interrupt level caused by IPv4 unicast or multicast traffic received via GREoIP or GREoMPLS tunnel if rate is high. If ingress interface is tunnel and egress is tunnel (MDT included) as well, then outer IP ToS of egress packet will be reset to 0x0.

  Conditions: The symptom is observed after a reload (under 10% probability), GRE tunnel must be in VRF:

```
#show running-config interface tunnel 513
interface Tunnel513
 vrf forwarding REN
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-mode
 tunnel source Loopback513
 tunnel destination 10.0.113.2 (via IP or MPLS interface)
 tunnel vrf REN
end
```

  To confirm hit:

```
#show vlan internal usage | include Tunnel513
4074 Tunnel513

#remote command switch show mls vlan-ram 4074 4074
```

  (If there is 256, the defect is present)

  Workaround: Reload the router.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

  Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

  Workaround: Only reloading the router resolves the issue.

- CSCtj53299

  Symptoms: Met corruption issue is observed.

  Conditions: This symptom occurs during OIF churn.

  Workaround: Use the **clear ip mroute** command for the problematic entry.

- CSCtj58943

  Symptoms: Standby RP reloads due to line by line sync failure for **encapsulation dot1q 1381** command:

```
encap dot1Q 1381
due to parser return error

rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync,
Reason: Configuration mismatch
```

  Conditions: Symptom occurs when issuing a configuration command under a sub-interface mode.

  Workaround: There is no workaround.

- CSCtj65553

  Symptoms: Static route that is installed in default table is missing.

  Conditions: Static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj72148

  Symptoms: A Cisco 7600 router might face an SP crash upon first reload after upgrade from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2. After successive reloads, the system functionality is restored.

  Conditions: This symptom is observed when upgrading from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2.

  Workaround: There is no workaround.

- CSCtj72730

  Symptoms: If an Enhanced Interior Gateway Routing Protocol (EIGRP) **address-family** configuration command is removed, any redistribution commands that refer to that address-family should also be removed. This defect documents a case where the redistribution command is not removed.

  Conditions: This issue occurs when the redistribution command is not removed after removing the corresponding EIGRP address-family configuration command.

  Workaround: Manually remove the redistribution commands that remain after the **address-family** command is removed.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj79085

  Symptoms: Multicast Forwarding Information Base (MFIB) entries are struck in NP HW_ERR MET-FULL:5, NP HW_ERR MET-ALLOC:6.

  Conditions: The above issue occurs during slot 7 reload, UUT-CE1 interface Flap, and UUT reload with traffic.

  Workaround: There is no workaround.

- CSCtj79750

  Symptoms: Multicast responses are not obtained.

  Conditions: After a Multicast Listener Discovery (MLD) join, multicast responses are not obtained.

  Workaround: There is no workaround.

- CSCtj79992

  Symptoms: Receiver end flooded in an MVPN scenario.

  Conditions: The symptom is observed even after stopping traffic.

  Workaround: There is no workaround.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

  Conditions: This issue occurs when summary address is advertised as follows:

  ```
  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
  ```

  Workaround: There is no workaround.

- CSCtj82401

  Symptoms: After rebooting Cisco ASR 1000 router, all adjacencies get detached and all calls fail.

  Conditions: If the configured default call-policy contains “na-carrier-id- table”, it will be converted to “na-dst-carrier-id-table”. During reboot, the “na-dst-carrier-id-table” is detected as an unrecognized command, therefore, that part of the config is rejected. This leaves the SBC in a state where all adjacencies are detached until the problem is corrected.

  Workaround: Manually add back “na-carrier-id-table” to the configuration after reloading the router. Deactivate and reactivate the SBC.

- CSCtj85858

  Symptoms: Coexistance of flat class-default shape policy-map (port level shape) and QoS on sub-targets (sub-interface, service instance, sessions and so on) is not supported on LowQ ES+.

  Conditions: This symptom occurs only on LowQ ES+.

  Workaround: There is no workaround.

- CSCtj86464

  Symptoms: Bundling does not occur with Distributed Link Fragmentation and Interleaving (dLFI) over ATM.

  Conditions: Bundle keeps flapping with dLFI over ATM.

  Workaround: There is no workaround.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

  Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

  Workaround: There is no workaround.

- CSCtj88825

  Symptoms: Fabric utilization goes high and drops are seen.

  Conditions: The symptom is observed when egress replication is configured with multicast. Global ICROIF index (0x02006) is programmed which causes high fabric utilization.

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: IOSd crashes when using the command **clear crypto session** on an EzVPN client.

  Conditions: Testbed setup:

  1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured.
  2. Use IXIA to generate 1Gbps traffic.
  3. Wait until all the SAs have been established and traffic is stable.
  4. Use CLI **clear crypto session** on EzVPN simulator.

  Workaround: There is no workaround.

- CSCtj94297

  Symptoms: “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

  Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

  Workaround: Use the **clear ip mroute** in the affected mroute.

- CSCtj94358

  Symptoms: SIP400 will pass the traffic through a previously configured VLAN on reconfiguring the **bridge-domain** command.

  Conditions: This symptom is seen with the egress interface that is a SIP400 with MPB configured.

  Workaround: Remove the “bridge-domain” configuration and then add the new “bridge-domain”.

- CSCtj94490

  Symptoms: Route Processor (RP) reloads after 30 RP switchovers.

  Conditions: This symptom occurs after 30 RP switchovers during 28000 PPPoEoA sessions while traffic is flowing.

  Workaround: There is no workaround.

- CSCtj94835

  Symptoms: Spurious memory access and tracebacks are seen on router reload.

  Conditions: The symptom is observed when the router is reloaded.

  Workaround: There is no workaround.

- CSCtj95032

  Symptoms: PIM packets are dropped at SIP400. As a result PIM neighborship is not formed between the CEs.

  Conditions: This symptom is seen when the egress interface is on SIP400 with bridging configured on it.

  Workaround: There is no workaround.

- CSCtj96489

  Symptoms: In a CISCO 7600 router, a freshly provisioned interface, or an interface which has been administratively no shut, belonging to non-default VRF, may fail to forward traffic.

  Conditions: This is a race condition and hence timing sensitive.

  Workaround: Another interface **shut/no shut** may help restore service.

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown. See Further Problem Description below.

  Workaround: There is no workaround. Only power cycle can remove the symptom.

  Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtj97360

  Symptoms: Punted datapaths are multicast flows GREoIP->DefaultMDT and GREoMPLS->Default MDT.

  Conditions: This symptom occurs with device bootup with IPv4-only VRF. After bootup IPv6 is enabled for VRF, which triggers the problem.

  Workaround: Do not have IPv6 AF and the mcast configurations in the same VRF.

- CSCtj97823

  Symptoms: The 32-byte topology names are not handled correctly on bootup.

  Conditions: This symptom occurs when 32-byte topology names are not handled correctly on bootup.

  Workaround: Use topology names shorter than 32 characters.

- CSCtk00398

  Symptoms: When receiving DHCPv6 SOLICIT from two clients with same DUID, DHCPV6 binds the Delegated-Prefix to incorrect client.

  Conditions: This symptom occurs when two clients are sending SOLICIT with same DUID.

  Workaround: There is no workaround.

- CSCtk00976

  Symptoms: File descriptor reaches the maximum threshold limit. You will be unable to save the configuration or do any file system related operation as file descriptors are exhausted. You will get "File table overflow" error.

  Conditions: The symptom is observed when running the **dir/recursive <>** command periodically using the ANA tool.

  Workaround: Do not run **dir/recursive <>** command if leaks are detected. Also, if it is running through ANA server polling, disable it.

- CSCtk02155

  Symptom: Attachment to the CHOC3 SPA console fails after seeing VC configuration command failures.

  Conditions: This symptom is seen with CHOC3 SPA on SIP200 or SIP400.

  Workaround: Reset the line card.

  Further Problem Description: The periodic process resyncs the IPC between the host and CHOC3 SPA. As this is not happening, we are not able to attach to the SPA console.

- CSCtk02661

  Symptoms: Bundles stop forwarding any traffic.

  Conditions: The symptom is observed when you move the SPA to a different bay on a SIP-400 and apply configurations on the new bay.

  Workaround: Reload spa on both ends.

  Alternate workaround: Unconfigure multilink before moving the SPA out.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it may be that per-user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

Conditions: This symptom is seen when LNS multilink is configured and negotiated for PPP/L2TP sessions per-user ACL downloaded for PPP users via radius.

Workaround: There is no workaround.

- CSCtk05652

  Symptoms: UDLD, that uses end-to-end across an AToM link, causes the CE link on one side to be put in err-disabled state.

  See the following topology:

  SW1 (CE) <-- PE-1 <-> MPLS cloud <-> PE-2 (7600 running 12.2(33)SRE2 --> SW2 (CE)

  UDLD err-disabling the port on SW2 is seen though the link is not unidirectional.

  Conditions: This issue is observed on Cisco IOS Release 12.2(33)SRE2.

  Workaround: Run Cisco IOS Release 12.2(33)SRD5.

- CSCtk06750

  Symptoms: IP-directed broadcast packets do not get forwarded by downstream router.

  Broadcast-source----R1---serial----R2-------rcr

  Conditions: When the serial link encapsulation is set to High-Level Data Link Control (HDLC), which is the default encapsulation, the layer2 HDLC frames are sent out with an incorrect address type in HDLC header. The downstream router does not recognize the payload as a broadcast packet and it does not forward it further as a directed broadcast packet.

  Workaround: Change the encapsulation to Point-to-Point Protocol (PPP) on the affected serial interfaces.

- CSCtk07369

  Symptoms: The buginf statement “draco2_fastsend: PAK_BUF_ON_OBL processing vlan” appears on the console.

  Conditions: This is displayed in certain cases, such as multicast replication.

  Workaround: There is no workaround.

- CSCtk07632

  Symptoms: Even with the filter option, traffic on a different VLAN on trunk port is getting spanned.

  Conditions: The symptom is observed when the filter vlan specified is not configured on the box.

  Workaround: Configure the vlan on the box, then configure it as SPAN filter vlan.

- CSCtk12252

  Symptoms: Priority 1, valid SONET controller network clock source does not get picked as an active clock source. Instead, the clock remains as FREERUN.

  Conditions: This issue occurs after reloading the router, when there is a valid but not present, priority 2 network clock source.

  Workaround: Perform a shut/no shut on the near-end Prio1 clock source SONET controller.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T and Release 15.1(01)S and with the following configurations:

  Router 1:

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 201.0.0.1 remote-as 200
 neighbor 201.0.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 200.0.0.1
ip route 201.0.0.1 255.255.255.255 10.0.12.2
ip route 201.0.0.1 255.255.255.255 10.0.120.2
```

Router 2:

```
interface Loopback200
 ip address 200.0.0.1 255.255.255.0
!
interface Loopback201
 ip address 201.0.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 200.0.0.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!
```

Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12708

  Symptoms: Router crashes when holdover clock source is deleted.

  Conditions: This symptom occurs when the holdover clock source is deleted.

  Workaround: There is no workaround.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: The symptom is observed when a subinterface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge domain. The traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, perform a shut/no shut on the interface.

- CSCtk30807

  Symptoms: A box that acts as a DHCP relay/server crashes when the DHCP service is toggled (no service dhcp/service dhcp).

  Conditions: This issue occurs when the box is also configured as ISG.

  Workaround: There is no workaround.

- CSCtk31340

  Symptoms: Cisco route processor (RP) crashes when a port-channel is removed and the member link is defaulted.

  Conditions: When a port-channel is removed (no int port-channel 200) and the member link is defaulted, the port-channel does not automatically remove the configurations on the member link. This crashes the route processor.

  Workaround: There is no workaround.

- CSCtk33682

  Symptoms: Storm control stops working.

  Conditions: The symptom is observed after a shut/no shut of the interface on an ES-20.

  Workaround: Remove/add the storm control command on the interface.

- CSCtk33821

  Symptoms: When polling VidMon metrics through SNMP during MSE intervals, no metric values are returned.

  Conditions: This symptom is observed when the MSE interval is being polled.

  Workaround: There is no workaround.

  Further Problem Description: When we get a MSE interval, the Cisco 7600 does not export the interval data to SNMP. During the MSE interval MRV will be - 100, CMM uses this value to determine the Media stop event. So it is critical to export the MSE interval to SNMP.

- CSCtk34026

  Symptoms: Adding, deleting and re-adding an access subinterface may sometimes cause loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create access subinterfaces from scratch.

- CSCtk36029

  Symptoms: The **match protocol** *icmp* command is not available under class map configuration.

  Conditions: This symptom is seen on the Cisco 7600 with ISG CoPP.

  Workaround: There is no workaround.

- CSCtk36064

  Symptoms: QoS policy-map with set CoS is applied on switchport interface of ES+ LC in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Conditions: This symptom is seen on a Cisco 7600 router. ES+ LC, QoS policy- map with set CoS is applied on switchport interface in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Workaround: There is no workaround.

- CSCtk36090

  Symptoms: Router crash at draco2_inband_dma_pak after a router reload with the following SRE image:

  s72033-adventerprisek9_dbg-mz.nightly_sre_2010-11-20

  Conditions: The symptom is observed following a router reload.

  Workaround: There is no workaround.

- CSCtk36377

  Symptoms: VRF ping fails for some of the VRFs after deleting and adding MVRFs.

  Conditions: This symptom is seen when adding and deleting MVRFs using a script.

  Workaround: Delete VRF and add it back.

- CSCtk37068

  Symptoms: Policing is not happening.

  Conditions: This symptom occurs when CoPP is enabled.

  Workaround: There is no workaround.

- CSCtk39301

  Symptoms: Tracebacks such as the following can appear on the RP:

  ```
  %C6K_MPLS_RP-STDBY-3-INFINITE_OCE: In label: 17 Invalid OCE  previous oce
  type: 29 prev
  ptr: 0x5648A2B0, next oce type: 29 next oce ptr: 0x0
  -Traceback= 42319368z 42322E68z 42BA0EF0z 438DCE10z 438D17F0z 405A209Cz
  405AC198z 405A7900z
  405EA768z 405EA9E0z 438D06B4z 438D0EE4z 438DAF98z 438FFE40z 422200D0z
  4222123Cz
  ```

  Conditions: The symptom is observed if there are more than eight or 10 ECMP paths for any prefix (i.e.: when there is a loadbalance object in the forwarding OCE chain).

  Workaround: Reduce the number of paths and do a **clear ip route** to re-initiate hardware programming.

- CSCtk47891

  Symptoms: Traffic might be blackholed when LC is reset, if Fast Reroute (FRR) is in use.

  Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk47960

  Symptoms: Large CLNP packets may be dropped when forwarded over SIP- 200/Flexwan2 module. Header Syntax errors may be recorded on receiving host.

  Remote side will generate the following:

  ```
  %CLNS-3-BADPACKET: ISIS: L1 LSP, packet (902) or wire (896) length invalid
  ```

  Conditions: This symptom is seen on Cisco 7600 switch with SIP-200 line card that is running Cisco IOS 12.2(33)SRD3 and later releases.

  Issue is seen when packets larger than 911 bytes are sent (Payload and Header).

  Workaround: If CLNS is only used for ISIS neighborships “no isis hello padding” can be configured to establish ISIS neighborship. For the LSP packets, configure lns-mtu 903 under router isis on the Cisco 7600 to make this work.

- CSCtk53463

  Symptoms: For configuring the **shape average** *cir value bc value* command currently across all platforms, *bc value* is limited by 4ms * *cir value*. The 4ms here represents minimum interval time for bursts. ES+ LC however can support interval value that is faster (smaller) than 4ms. This has been expected behavior with exception of ES+ LC.

  Conditions: Currently all platforms restrict interval time for shape from going below 4ms.

  Workaround: There is no workaround.

- CSCtk54318

  Symptoms: VC creation fails on disabling and re-enabling the card for SIP-400 with 4XT3E3 SPA with below messages on console:

  ```
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed -
  fr_npc_vc_add: vc creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 0
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed -
  fr_npc_vc_add: vc creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 1023
  ```

  Condition: This issue is seen when the below commands are executed on a T3 serial interface of the SPA 4XT3E3 configured as DTE with frame relay encapsulation:

  no card type t3 *slot bay*
  card type t3 *slot bay*

  Then unconfigure and reconfigure frame relay enacapsulation.

  Workaround: Reload the SPA.

- CSCtk54431

  Symptoms: When a Cisco ASR 1000 BRAS receives SOLICIT IA-PD from CPE, but no Delegated-IPv6-Prefix has been received from Radius, currently, NO reply is sent to the CPE. An Advertise with option “NoPrefixAvail” should be sent instead (RFC 3633).

  Conditions: This symptom is seen when CPE requests IA-PD, but BRAS does not have any Delegated-IPv6-Prefix.

  Workaround: There is no workaround.

- CSCtk55382

  Symptoms: A SPA-OC192POS-VSR or SPA-OC192POS-XFP may fail boot diagnostic test.

  Conditions: The symptom is observed when Control Plane Policing (CoPP) is configured on the system. The diagnostic test that fails is the “TestACLPermit” test displayed in “show diagnostic result”. The output of “show module” will indicate a “Minor error” on the subslot.

  Workaround: Before a system reload or module reset, disable the CoPP feature. After the module is booted, CoPP can be enabled again.

- CSCtk57049

  Symptoms: After access interface flap on encap PE in MVPN setup, the traffic is not sent over data MDT even though the VRF selects the data MDT for encap.

  Conditions: This symptom is seen after access interface flap on encap PE in MVPN setup, the traffic is not sent over data MDT even though the VRF selects the data MDT for encap.

  Workaround: There is no workaround.

- CSCtk59347

  Symptoms: CPU is busy and console is locked up for minutes after entering the **clear counter** command.

Conditions: This symptom occurs with a large scale configuration with hundreds of interfaces and service groups configured on the system.

Workaround: Instead of clearing all counters of all interfaces, clear the counters of specific interfaces as needed.

- CSCtk67658

  Symptoms: Traceback and infrequent crash of the new active are seen when SSO is performed on a router.

  Conditions: This symptom occurs when SSO is performed on a router.

  Workaround: There is no workaround.

- CSCtk68647

  Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

  Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

  Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk75389

  Symptoms: PFR fallback interface on Cisco ASR 1000 platform fails to remain in inpolicy.

  Conditions: The issue is seen on Cisco ASR 1000 platform and only with ATM interface.

  Workaround: There is no workaround if ATM interface is used on the Cisco ASR 1000 platform.

- CSCtk76190

  Symptoms: The RSP/SUP fails to switchover automatically when the “TestSPRPInbandPing” fails for more than 10 instances.

  Conditions: The symptom is observed when the “TestSPRPInbandPing” fails for more than 10 instances.

  Workaround: There is no workaround.

- CSCtk83760

  Symptoms: Met updates from SUP are reaching Cisco 67xx DFC cards.

  Conditions: This symptom is observed during OIF churn. This is not reproduced locally, and the fix is put in as a sort of preventive mechanism.

  Workaround: There is no workaround.

- CSCtk98030

  Symptoms: After replacing an ES20 line card with an ES+ line card or vice versa in the same slot, some service groups reject new members to join if the old line card had ethernet service instances in these groups. Similarly, a named EVC rejects new ethernet service instances if it had association with the old line card. The named EVC cannot be deleted, complaining that it still has service instances.

  Conditions: The symptom is observed if an ES20 line card has been replaced with an ES+ line card or vice versa in the same slot. The old line card had ethernet service instance members in some service groups and/or named EVCs. The old associations between ethernet service instances and service groups or named EVCs are not cleaned up properly, blocking new association to these groups and EVCs.

Workaround: Configure new service groups and named EVCs with same configuration as the problematic ones. Abandon the use of the old groups and EVCs. Assign ethernet service instances from the new line card to the new groups and EVCs.

- CSCtl03100

  Symptoms: Router crashes due to severe memory fragmentation.

  Conditions: This symptom occurs with the following configuration:

  - 6000 series scalable EoMPLS
  - 500 sw-based EoMPLS
  - 2.5k VPLS instances
  - 100 vrfs(50 L3VPN, 30 MVPN, and 20 6VPE)
  - QOS policies on around 1600 interfaces.

  Workaround: There is no workaround.

- CSCtl05926

  Symptoms: Packets of size exceeding MTU are dropped with the following error messages:

  ```
  %CONTROLLER-3-TOOBIG: An attempt made to send giant packet on  \
  GigabitEthernet7/3/1 (1491 bytes from 10010046, max allowed 1476
  ```

  Conditions: This symptom is observed when the outgoing interface is on SIP400.

  Workaround: There is no workaround.

- CSCtl05979

  Symptoms: In SSO mode, PPPoE sessions with PAC2 ISG service are replicated to Standby RP, with policy-maps missing on Standby RP. PAC2 service should poison the PPPoE session.

  Conditions: This symptom is observed in SSO mode, when PPPoE sessions with PAC2 ISG service are established.

  Workaround: Use dummy ISG service applied from RaBaPol to force poisoning.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- CSCtl08601

  Symptoms: Unconfiguring DHCP pool hangs the console.

  Conditions: This symptom is observed when “no service dhcp” is issued prior to unconfiguring the pool.

  Workaround: There is no workaround.

- CSCtl10395

  Symptoms: Control Plane Policing (CoPP) stops dropping packets in hardware on a Cisco 7600 series router after double switchover.

  Conditions: This symptom occurs on the Cisco 7600 platform when CoPP is configured on the router and SSO (HA Switchover) is done twice.

  Workaround: Remove and reconfigure the CoPP.

- CSCtl18652

  Symptoms: After replacing an ES20 with an ES+ line card on the same slot, or vice versa, adding ethernet service instance members from the new line card to an existing service group that was associated with the old line card may cause a reload of the standby RP in SSO mode. This is due to stale configuration on the standby RP.

  Conditions: An ES20 line card has been replaced by a different type of line card or vice versa, on the same slot. New members are assigned to a service group that had members from the old line card. There is a standby RP in SSO mode.

  Workaround: Create a new service group with the same configuration as the existing group and assign new members to the new group. Abandon the use of the old group.

- CSCtl19347

  Symptoms: On configuring additional bundles, LC crashes. This occurs with SIP- 400 when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Conditions: This symptom occurs when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl41921

  Symptoms: There is a traffic duplication.

  Conditions: This symptom occurs with bootup with scale having 2000 sLSPs.

  Workaround: Do a shut/no shut on the tunnel.

- CSCtl42358

  Symptoms: A Cisco ASR 1000 series router crashes after “no atm sonet overhead j1” command on an ATM interface.

  Conditions: This symptom occurs on a Cisco ASR 1000 series router on an ATM interface.

  Workaround: There is no work around.

- CSCtl46703

  Symptoms: T1/E1 tributary on Prowler SPA stays down occasionally after LC/SPA is reloaded.

  Conditions: This symptom occurs after LC/SPA is reloaded.

  Workaround: Reconfigure clock configuration (e.g. vtg 1 t1 1 clock source line/internal) on the affected T1/E1.

- CSCtl46903

  Symptoms: VLAN mapping or translation feature does not work on ES+, when the port is configured as L2 switchport.

  Conditions: This symptom occurs when the port is configured on L2 switchport.

  Workaround: Configure the feature under EVC framework or L2 switchport on LAN cards.

- CSCtl50930

Symptoms: For some sip messages (for example, OPTION), SBC will assert failure when call goes through VRF.

Conditions: This symptom only happens on 1001/1002/1004 non-redundant mode.

Workaround: Configure redundant mode SSO.

- CSCtl55828

  Symptoms: LDP/OSPF PDUs get dropped when line rate traffic is running on the Interface in case the link is over subscribed.

  Conditions: This symptom occurs with the following Hardware and software:

  Hardware - ES+ LC

  Software - Cisco IOS Releases 15.0(1)S, 15.0(1.1)S, 15.1(1)S Link over subscription, output drops at the MPLS interface.

  Workaround: There is no workaround.

- CSCtl58623

  Symptoms: MCP XE32 build breaks.

  Conditions: This symptom occurs in all conditions.

  Workaround: There is no workaround.

- CSCtl69609

  Symptoms: When bringing down the shortest route, traffic blackholing occurs in MLDP on one of the OIF.

  Conditions: This condition occurs in MLDP and branch point combination.

  Workaround: There is no work around.

- CSCtl74301

  Symptoms: INBOX Stateful Switch Over (SSO) does not work on Cisco ASR 1006 routers in RLS 3.2(8). When this occurs, SSO drops signaling and RTP.

  Conditions: This symptom occurs for INBOX SSO. This happens when SIP binds with the loopback address for control.

  Workaround: There is no workaround. Unless required by your network architecture, do not use loopback address for control bind.

- CSCtl83053

  Symptoms: Unable to change the shaper rate with ANCP port up messages.

  Conditions: This symptom occurs with the Cisco ASR 1000 series router with QoS and ANCP enabled.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(1)S. All the caveats listed in this section are open in Cisco IOS Release 15.1(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCth08313

  Symptoms: The following is seen during online operations:

  ```
  : %SYS-SP-2-GETBUF: Bad getbuffer, bytes= 24616
  -Process= "IPC Periodic Timer", ipl= 0, pid= 24
  -Traceback= 81745F8 81D19E8 8BEAD94 8BEB5C4 853BAD4 8527704 854CE24 82AE1B0 82AE2E8
  855E454 835AFD0 83552E8
  ```

  Or

  ```
  IPC: Sending Big IPC msg to Driver MSG: ptr: 0x152CDAC8, flags: 0x14328, retries: 1,
  seq: 0x2016C68, refcount: 2, rpc_result = 0x0, data_buffer = 0x14FB3084, header =
  0x78730658,
  data = 0x78730678 || HDR: src: 0x216001E, dst: 0x2010000, index: 0, seq: 27752, sz:
  1808,
  type: 14209, flags: 0x1608, ext_flags: 0x0, hi: 0x1B622B, lo: 0x36C456 || DATA: 00 00
  00 06
  0E 19 00 08 00 00 00 00 00 00 03 12 00 00 00 00 89 00 00 00 00 00 00 00 00 00 06 E8 00
  00 00 01 11 9E 04 34 04 60 08 00 00 01 00 20 6E 00 67 05 EF E8 00 06 00 00 00 20 00 00
  00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16
  ```

  Conditions: This symptom is seen either after boot of the router or after failover on a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCth08800

  Symptoms: Multicast traffic gets replicated to EVCs, which have not joined a multicast feed.

  Conditions: This symptom is seen when we have multiple EVCs under a single bridge-domain service with active multicast receivers spread across the EVCs. Upon disabling and re-enabling snooping on bridge-domain VLAN, multicast gets wrongly replicated by NP on Excalibur.

  Workaround: Reconfigure the physical interface carrying the EVCS.

- CSCti08301

  Symptoms: The SPA gets reloaded due to Semaphore hog and heartbeat failures.

  Conditions: This symptom occurs when member links of a multilink bundle is added/removed or moved across multilink bundles while sending traffic at bigger frame size and higher rate.

  Workaround: There is no workaround.

- CSCti08740

  Symptoms: When network payload loopback is followed by remote line fdl ansi loopback, the remote fdl ansi fails.

  Conditions: This symptom happens when network payload loopback is followed by remote line fdl ansi loopback.

  Workaround: Do the remote line fdl ansi alone.

- CSCti17802

  Symptoms: The following log message may be incorrectly displayed to prompt the user to issue the **issu runversion** command in cases where the ISSU upgrade has been aborted due to an error.

  ```
  "ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please issue the runversion
  command"
  ```

  Conditions: Wrong message is shown when ISSU is aborted after issuing the **issu loadversion** command. This behavior has no functional impact.

  Workaround: There is no workaround.

- CSCti20319

  Symptoms: After ISSU, the LTL entry corresponding to L3 receiver on CFC in egress replication mode does not have the OIF slot programmed in platform entry on SP.

  Conditions: This symptom is seen after ISSU runversion. It is not seen after SSO.

  Workaround: Do a module reset of the egress CFC card.

- CSCti22462

  Symptoms: On adding more than 18 slaves with delay request rate at 32 PPS to a master session, existing slaves start flapping.

  Conditions: This symptom occurs with a setup with more than 18 slaves connected to a master session with delay request rate at 32 PPS.

  Workaround: Reduce the delay request rate on the slave side. Keep number of slave sessions connected to a master of less than 18.

- CSCti23169

  Symptoms: Redistribution of EIGRP into BGP at the PE creates an external route at the CE at the other end.

  Conditions: When we redistribute EIGRP into BGP at the PE and the EIGRP has a network that is actually a loopback interface on this PE, we see the other end CE shows it as an external route. The specific condition for this is only when this network is the first network statement applied in the EIGRP. For example, see the following:

  ```
  net 10.0.0.0 is the subnet for the loopback interface on the PE and net
  192.168.0.0 is the other interface network address which has a neighbor at
  the other end. We have EIGRP redistributed into BGP and we are now
  configuring EIGRP as
  router eigrp
  network 10.0.0.0
  network 192.168.0.0
  ```

  In this condition we see an external route created for 10.0.0.0 network at the other CE. If we reverse the network statement order, we do not see this issue. Also when we use the **no network** *10.0.0.0* command and reenter the network statement, we do not see the issue.

  In any live network, such configuration will never occur. The customers will never try to add the loopback address of a PE and send it to the other CE over EIGRP PE-CE network.

  Workaround:

  1. Reverse the network statements
  2. Do a **no network** and **network** for that network.

- CSCti27214

  Symptoms: BFD/Routing flaps, and packet loss is seen.

  Conditions: This symptom is seen when Standby RP is coming up to life.

  Workaround: Disable both QoS (containing NBAR) and NBAR protocol discovery from under all interfaces.

- CSCti40325

  Symptoms: Radius retransmit timeout happens (roughly) at half the timeout configured by the **radius-server timeout** *timeout* command. For example, for the default timeout value of 5 seconds, timeout happens at 2 to 3 seconds. For higher values, for example 20, timeout happens at around 10 seconds.

  Conditions: This symptom is seen when radius server is used for AAA.

Workaround: There is no workaround.

- CSCti47426

  Symptoms: NAT address is consistently added in the FIB table as a receive adjacency. This results in packet getting incorrectly routed.

  Conditions: This issue is seen with static NAT such that NAT source address is same as destination address.

  Workaround: There is no workaround.

- CSCti66996

  Symptoms: SIP400 crash is seen on reloading the chopper SPA, which has MLP bundles configured.

  Conditions: This symptom is seen when swapping the member links across bundles and reloading the SPA. The crash is seen sometimes.

  Workaround: There is no workaround.

- CSCti78950

  Symptoms: Traffic is sent to RP for unresolved entries.

  Conditions: This symptom occurs when the remote is not responding to ARP.

  Workaround: There is no workaround.

- CSCti81076

  Symptoms: PVC creation fails on controller with the following message:

  ```
  ACRPVCADD : PVC creation fails
  ```

  Conditions: This issue is seen with the following steps:

  1. Add working and protect controller to ACr group.
  2. Configure virtual controller for ATM and create L2VP on ATM-ACR interface.
  3. Shut the working controller.
  4. Remove atm config from virtaul controller and configure again.
  5. Do “no shut” on the working controller.

  Workaround: Configure when controllers are UP.

- CSCti82670

  Symptoms: An RSP will crash when the CFM automated test script (consisting of 53 tests) is run twice in succession.

  With SUP720, the crash is seen with a single run.

  Conditions: The automated test script must be run on 3 connected routers.

  Workaround: Adding a **no shut** on UUT interface with UP- MEPS before doing the LeakConfig seems to prevent the crash and provide a clean run.

  Further Problem Description: Other problems observed are:

  - The CFM MIB will return infinite results for getmany.
  - A **show** command will crash the router.

- CSCti87639

  Symptoms: Standby RP reloads due to config out of sync or keepalive failure in RPR mode.

  Conditions: This issue is observed while running NBAR scripts or sometimes with no activity on box. It cannot be reproduced manually.

Workaround: Operate in SSO mode.

- CSCti87947

  Symptoms: All the police profiles applied on Service groups on a port-channel interface do not get cleared on deleting the port-channel interface.

  Conditions: This symptom occurs with scale configurations and ingress policers applied on SG on port-channel interface.

  Workaround: Line card online insertion and removal (OIR) solves the problem.

- CSCtj05670

  Symptoms: When doing SSO with scaled mLDP configuration, path set for some of the VRFs are not configured.

  Conditions: This issue only occurs when configuring mLDP on 100 VRFs with 100 receivers.

  Workaround: There is no workaround.

- CSCtj19150

  Symptoms: Service policy applied on VP not seen on standby RP after doing APS switchover Issue is seen only in scale environment and when Both Active and protect controllers are on different LCs.

  Conditions: The issue will be seen under the following conditions:

  1. Configure ACR on both working and protect controllers (on different LCs).
  2. Configure virtual controller for ATM.
  3. Configure 100 ATM PVPs and apply service policy.
  4. Do APS switchover.

  Workaround:

  1. Have both working and protect controller on same LC.
  2. After APS switchove remove and again apply service policy.

- CSCtj22784

  Symptoms: A service-group is not getting configured.

  Conditions: This symptom is seen when a service-group is not getting configured on scaled configurations.

  Workaround: There is no workaround.

- CSCtj24811

  Symptoms: A Cisco ASR 1000 router may crash when RSVP aggregation feature is configured and FLR is triggered.

  Conditions: This symptom is seen when usage of RSVP aggregation feature and FLR is triggered.

  Workaround: There is no workaround.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there is not traffic match in the class.

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

Workaround: Do not use WRED subclass transmit packets/bytes counters for ES+ line card on Cisco 7600 router.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1
    redistribute connected
    no redistribute connected
  ```

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj35914

  Symptoms: In a setup with primary CEM PW and a backup configured, the traffic flows in the backup path when the primary is still up.

  Conditions: Reload the module on the peer PE, when the primary path/controller is down. Allow the backup path to come up when primary path is still down. Bring up the primary path now, the traffic will not be switched to the primary path. The traffic still flows in the backup path, though the primary path is up. The traffic does not switchover to primary, even if the backup path goes down.

  Workaround: Reset the module on the peer PE again when the primary controller/path is up.

- CSCtj44160

  Symptoms: The “failed to reparent member to new group” error message is seen as soon as flat SG is applied on subifs and after that, it gets rejected.

  Conditions: This symptom is seen in bringup sessions from subifs having HQoS policy applied on session control policy and attach flat SG to the subifs.

  Workaround: There is no workaround.

- CSCtj47086

  Symptoms: If a connected route that is also owned by EIGRP or OSPF is replicated from one routing table to another, any route-map that is applied when redistributing the route into EIGRP will not work properly if the source specified during redistribution is anything other then connected (for example EIGRP or OSPF).

  Workaround: Make sure to specify the source as EIGRP or OSPF instead of connected when redistributing the replicated routes.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

  Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

  Workaround: Only reloading the router resolves the issue.

- CSCtj52969

  Symptoms: The following message may be observed when issuing the **show issu state detail** command after performing an **issu loadversion** operation:

  ```
  %ISSU_PROCESS-3-IPC_AGENT: Failed to send; error code [ timeout ]
  ```

  Conditions: This message may be observed when issuing the **show issu state detail** command after performing an **issu loadversion** operation. This message may also be observed if the **show issu state detail** command is given while the standby is reloading for any other reason.

  Workaround: When the standby is booting up after issuing the **issu loadversion** command, do not use the **show issu state detail** command until the standby is completely up. There is no functional impact, except that for a small period of time (a few seconds), the standby information is temporarily unavailable.

- CSCtj58686

  Symptoms: Difference is seen in subclassification for Kazaa over http and Kazaa over non80 traffic.

  Conditions: This symptom is seen with difference in subclassification for Kazaa over http and Kazaa over non80 traffic.

  Workaround: There is no workaround.

- CSCtj64755

  Symptoms: Console hangs for 4 to 5 minutes when IMA configurations are removed from the virtual controller with scale.

  Conditions: This issue is seen when IMA interface is configured for scale. Console hangs when IMA configuration is removed from virtual controller by “no vtg 1 t1 ima-group”.

  Workaround: There is no workaround.

- CSCtj93845

  Symptoms: Memory leak in ACL is observed with PBR configuration.

  Conditions: This memory leak is observed when 200 application traffic classes are configured using PfR, and traffic is left running on the testbed for sometime.

  Workaround: There is no workaround.

- CSCtj94188

  Symptoms: After LC OIR the red AIE peer and AIE Peer id become the same. This causes the PWs to go down.

  Conditions: LC OIR causes the red AIE peer id and AIE peer id to become same.

  Workaround: Clear xconnect all reprovisions the PWs and the issue is not seen.

- CSCtk05205

  Symptoms: FMAN-FP crashes with scaled traffic.

  Conditions: This symptom is seen with a plain firewall and is receiving scaled SMTP traffic that is sent by Avalanche tool with different source ip addresses in the same subnet.

  Workaround: Using the **parameter-map type inspect** command and restricting the maximum scaling numbers, we can avoid the crash, but scaling number will be less.

- CSCtk10381

  Symptoms: Met3 is being set to 0 on doing SSO with mLDP intranet configurations.

  Conditions: This symptom is seen with MVPN session in data MDT mode and doing SSO switchover.

Workaround: Clear ip mroute of the affected steams.

- CSCtk13121

  Symptoms: Router crashes inconsistently when doing pings.

  Conditions: This symptom is seen with router crashing inconsistently when doing pings.

  Workaround: There is no workaround.

- CSCtk13169

  Symptoms: Ping does not pass through in dLFI over ATM with sip-200+sip-400.

  Conditions: This symptom is seen when ping does not pass through in dLFI over ATM with sip-200+sip-400.

  Workaround: There is no workaround.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: When a sub-interface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge-domain, the traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, performing a **shut/no shut** on the interface restores all traffic.