Caveats for Cisco IOS Release 15.1(3)S

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:

Open Caveats—Cisco IOS Release 15.1(3)S6

Cisco IOS Release 15.1(3)S6 is a rebuild release for Cisco IOS Release 15.1(3)S.

- CSCtn00145

  Symptom: Standby sup reloads on issuing the **no ip route** command.

  Conditions: This symptom is observed when static route statements present on the active and is missing on the stand-by. Perform these steps to recreate the issue:

  1. Configure a static route with an interface dependency (eg: ip static route 1.1.1.0 255.255.255.0 eth 0/0).
  2. Shutdown the Hardware Module/SPA corresponding to that interface. When the hardware module/SPA corresponding to that interface is shutdown, the static route entry is hidden from the configuration.

3. Reload the stand-by. When stand-by comes up, it performs a bulk sync to the running configuration of master. However the static routes which are HIDDEN, won't be present in the running configuration of master and hence will not be created in stand-by.
4. Bring up the hardware module/SPA. As this is still treated as OIR, the HIDDEN flag will be removed from the static routes and other related configurations will now be part of running configurations in the master. However these static routes are not present in stand-by as these information is lost due to reload and there will not be a disclosure of routes in standby and standby will be missing these static routes.
5. User executes no ip route. The route will be removed from master but as standby doesn't have these routes, it will result in a PRC failure leading to a standby reload.
6. Stand-by comes up after the reload. Now, it will have the entire configuration along with static routes in sync as the unhidden static routes are now part of the running configurations that are synced to standby

Workaround: Reloading the standby (most likely in a maintenance window) is the only way to sync missing ip route statements.

Resolved Caveats—Cisco IOS Release 15.1(3)S6

Resolved Caveats—Cisco IOS Release 15.1(3)S6

Cisco IOS Release 15.1(3)S6 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S5a but may be open in previous Cisco IOS releases.

- CSCsl38246

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

  ```
  %MWAM-DFC3-0-CORRECTABLE_ECC_ERR: A correctable ECC error has occurred,
  A_BUS_L2_ERRORS: 0x0, A_BUS_MEMIO_ERRORS: 0xFF, A_SCD_BUS_ERR_STATUS: 0x80DC0000
  ```

  This can potentially lead to watchdog invocation and a subsequent crash.

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

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

- CSCtj24692

  Symptom: NVRAM configuration file gets corrupted when a chassis is power cycled without a graceful shutdown.

  Conditions: This symptom is observed when you power cycle an ASR chassis without graceful shutdown.

  Workaround: Shutdown chassis using **reload** command and make sure RP gets to rommon mode before power cycling the chassis.

- CSCtj61284

  Symptom: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

Workaround: There is no workaround.

- CSCtl18571

  Symptom: On a Cisco 7600 series router with etherchannels configured, the **show etherchannel load-balance module** *x* command shows VLAN included even though the excluded VLAN has been configured globally using the **port-channel load-balance** *algorithm* **exclude vlan** command.

  Conditions: This symptom occurs when the system is operating in pfc3c or pfc3cxl mode with CFC and DFC card without per module load-balance.

  Workaround: This is an issue with the **show** command. The algorithm itself is not affected. The load-balancing algorithm is applied correctly as configured globally.

- CSCtq26296

  Symptom: Cisco router crashes with DLFI configurations.

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

  Workaround: There is no workaround.

- CSCtr88785

  Symptom: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts02627

  Symptom: The **show mac-address-table** command displays invalid/incomplete port list for entries learned on VPLS Bridge Domain.

  It is observed that port-channel “Po1” is displayed as “Po”, and the Virtual Circuit IDs are missing in the port list of the mac-address-table entries. This is a display issue.

  Conditions: This symptom is observed only with mac-address-table entries that are learned on VPLS Bridge Domain VLAN.

  Workaround: There is no workaround.

- CSCts13720

  Symptom: When static pseduowires are configured with VCCV BFD, some of the VCs may not come up.

  Conditions: This symptom occurs when a static pseudowire is configured with VCCV BFD.

  Workaround: For the VCs that are DOWN, issue the **clear xconnect peer** *peer-ip-address* **vcid** *vcid value* command to bring the VC back UP.

- CSCts22336

  Symptom: The Cisco router may reload due to a bus error when configured with DMVPN.

  Conditions: This has been seen on Cisco IOS Release 15.1M and Cisco IOS Release 15.2T. The crash only occurs on devices that have at least one point-to-point GRE Tunnel interface configured with NHRP enabled. This type of interface is typically used to interconnect DMVPN hubs with point-to-point extension links.

  Workaround: Reconfigure the point-to-point GRE extension tunnel as an mGRE interface: -

  ```
  shutdown - no tunnel destination - tunnel mode gre multipoint - no shutdown.
  ```

The Tunnel interface must also have a static NHRP entry for the DMVPN peer, of the form:

```
ip nhrp map remote-tunnel-address remote-NBMA-address
```

where remote-NBMA-address is the same address that was configured in the "tunnel destination" statement. On an extension link, this configuration should typically already be present.

- CSCts60458

  Symptom: There is a memory leak in PfR MIB.

  Conditions: This symptom occurs when PfR is configured.

  Workaround: Reload the RP to free the memory for IOSd

- CSCtt21701

  Symptom: ASR CUBE is getting crashed when the endpoint tries to change IP address and media port in an early dialog UPDATE, but for codec change it works fine.

  Conditions: The crash is seen only when SDP passthrough is enabled and IP address and media port are being changed by an early dialog UPDATE.

  Workaround: Without SDP passthrough it works fine.

- CSCtw45592

  Symptom: The **ntp server** *DNS-name* command is not synced to the standby. When the **no ntp server** *hostname* command is issued later on the active, the standby reloads because the configuration was not added.

  Conditions: When the device is reloaded or when the DNS name is not resolved, the configuration is not added. It is seen after the standby sync failure, then issuing the **no ntp server** *hostname*.

  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations. The IP/IPv6 address can be found by pinging the hostname.

- CSCtx82890

  Symptom: After removing the encapsulation on MFR member interface, tracebacks are observed.

  Conditions: This symptom is observed when serial interface is configured with FR MLP configuration.

  Workaround: There is no workaround.

- CSCty12641

  Symptom: CFM ethernet ping fails with 7600 as the remote MEP end.

  Conditions: This symptom is observed after remote CFM over Xconnect MEPs with MEPs terminating on 7600 and having ESM20 LC.

  Workaround: There is no workaround. Consider using ES+LC.

- CSCty51453

  Symptom: Certificate validation using OCSP may fail, with OCSP server returning an "HTTP 400 - Bad Request" error.

  Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T2 and later.

  Workaround 1: Add the following commands to change the TCP segmentation on the router:

  ```
  router(config)# ip tcp mss 1400 router(config)# ip tcp path-mtu-discovery
  ```

  Workaround 2: Use a different validation method (CRL) when possible.

- CSCty77441

  Symptom: Memory leaks are observed after unconfiguring the BFD sessions.

  Conditions: This symptom occurs after the BFD sessions are unconfigured.

  Workaround: There is no workaround.

- CSCtz33778

  Symptom: MDT remains in deleted state after several successive mdt removes/adds under the VRF.

  Conditions: The issue is seen when remove and add mdt is done quickly for multiple VRFs through a script.

  Workaround: Remove and re-add the VRF.

- CSCua24676

  Symptom: The VRF to the global packet's length is corrupted by -1.

  Conditions: This symptom occurs when the next-hop in the VRF is global and recursive going out labeled. This issue is seen from Cisco IOS Release 15.0(1)S3A onwards, but is not seen in Cisco IOS Release 15.0(1)S2.

  Workaround: Use the next-hop interface IP instead of the recursive next-hop.

- CSCua61201

  Symptom: Unexpected reload with BFD configured.

  Conditions: When a device is configured with BFD it may experience unexpected reloads.

  Workaround: There is no workaround.

- CSCua96354

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

  Conditions: This symptom is observed with the following commands:

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

  Workaround: There is no workaround.

- CSCub40547

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

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

  Workaround: Remove vidmon configuration.

- CSCuc05929

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

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

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

- CSCuc08477

  Symptom: All EOS and non EOS entries are missing for mLDP labels in the mid/bud node.

  Conditions: This symptom may occur due to random path flap mLDP tree changes.

  Workaround: Removing and adding the mLPD tree will trigger re-programming.

- CSCuc44306

  Symptom: The IPv6 HbH packets get punted to RP as a result of HbH rate-limiter not working.

  Conditions: This symptom is observed when IPv6 HbH packets hit the bridged interface on SIP400/SIP200 with IPv6 HbH rate-limiter configured.

  Workaround: There is no workaround.

- CSCuc55634

  Symptom: IPv6 static route cannot resolve the destination.

  Conditions: This symptom is observed under the following conditions:

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

  Workaround: There is no workaround.

- CSCuc78328

  Symptom: SP crashes followed by an RP reset.

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

  Workaround: There is no workaround.

- CSCud22222

  Symptom: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.

  Conditions: This symptom may occur if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.

  Workaround: Configure metric-style wide for both levels (by default).

- CSCud24084

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

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

  Workaround: Delete and add the affected VRF.

- CSCud24806

  Symptom: Compared to V1 ATM SPA, V2 SPAs are having more latency and bad bandwidth partition.

  Conditions: The symptom is observed under the following conditions:

  1. V2 SPA configured in L3 QoS mode.

2. Policy map contains “no priority queue”.
3. Policy map has more than one QoS class.
4. Each class has a WRED profile configured.

Workaround: While using a policy-map with a WRED profile, use the drop-probability value as 8. This improves the partition.

- CSCud28541

  Symptom: SP crashes on doing **no mpls ip** followed by **shut** on port-channel acting as core link for scaled VPLS and EoMPLS setup.

  Conditions: In case of VPLS going over port-channel protected by IP-FRR, when the port-channel is shut the AToM VC is going down and getting created again. Also the PPO object is getting created afresh. The VC going down is not handled for VPLS case and AToM VC’s pointer are still stored in IP-FRR’s EoMPLS list which is getting access and hence crashing.

  Workaround: There is no workaround.

- CSCud41058

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

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

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

- CSCud57841

  Symptom: When the Ethernet SPA with Catskills SFPs (GLC-SX-MMD /GLC-LH-MMD) is reloaded, the SPA could go out of service with the following error message:

  ```
  %SMC-2-BAD_ID_HW: SIP0/0: Failed Identification Test in 0/0 [7/0]
  ```

  Conditions: This symptom occurs when the Ethernet SPA is booted with the Catskills SFPs (GLC-SX MMD/GLC-LH-MMD). The defect could be hit during both reload and initialization.

  Workaround: Boot the Ethernet SPA without the Catskills SFPs and insert the Catskills SFPs after the Ethernet SPA has completely booted.

- CSCud66955

  Symptom: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to the fast bouncing of up or down 10s, after the interface is brought up.

  Conditions: This symptom is observed in E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud90950

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

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

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

- CSCue01146

  Symptom: SNMP GET fails for VPDN-related MIB.

Conditions: This symptom occurs while receiving an SNMP GET for the MIB before all VPDN configurations are applied.

Workaround: Reload the Cisco router.

- CSCue02242

  Symptom: VLAN-RAM is programmed with VPN as 0. Traffic destined to a particular vpnid is dropped though it comes on a proper VLAN.

  Conditions: This symptom occurs during P2P scaled configuration when the router boots up and notices the VLAN-RAM is programmed with vpnid 0.

  Workaround: Reload the line card.

- CSCue05492

  Symptom: The DHCP snooping client ignores the IPC flow control events from CF.

  Conditions: This symptom is observed when CF gives flow control off event and the DHCP snooping client does not handle it.

  Workaround: There is no workaround.

- CSCue18133

  Symptom: The Cisco 7600 Router crashes at show_li_users.

  Conditions: This symptom is observed under the following conditions: In li-view, create an username: lawful-intercept and li_user password: lab1. Then, attempt its delete by “no username li_user”. Later, show users of LI.

  Workaround: There is no workaround.

- CSCue31321

  Symptom: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.

  Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.

  Workaround: Set “term len 0” before running the **how ip cef ... detail** command.

- CSCue32450

  Symptom: Filtering based on L4 ports does not happen for redirection to CE.

  Conditions: This symptom occurs when the WCCP service uses a redirect-list and this ACL has its first entry as a “deny”.

  Workaround: Make the first entry in the redirect-list ACL as a “permit”.

- CSCue36197

  Symptom: The Cisco 7600 router may crash while performing the NSF IETF helper function for a neighbor over a sham-link undergoing NSF restart.

  Conditions: This symptom occurs when a router is configured as an MPLS VPN PE router with OSPF as PE-CE protocol. OSPF in VRF is configured with a sham-link and a neighbor router over a sham-link is capable of performing an NSF IETF restart on sham-links.

  Note: This problem cannot be seen if both routers on sham-link ends are Cisco IOS routers.

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

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

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

- CSCue43050

  Symptom: VLAN-RAM is programmed with VPN 0. PIM neighborships of random sessions (10-12 out of 30) go DOWN.

  Conditions: This symptom occurs when MVPN is configured with 30 L3VPN sessions. When there is a boot up, PIM neighborships of random sessions (10-12 out of 30) go DOWN.

  Workaround: Remove and add the VRF configuration for these MVPN sessions.

- CSCue44554

  Symptom: Traffic stops forwarding over port-channels configured with FAST LACP after an RP switch over.

  Conditions: This symptom occurs after an RP fail over.

  Workaround: A shut/no shut interface will help recover.

- CSCue47586

  Symptom: For an MGRE tunnel, internal VLANs are not allocated in the standby supervisor.

  Conditions: The symptom is observed when an HA router boots up with MGRE tunnel configurations. Internal VLANs are not allocated in the standby supervisor due to a sync issue during bootup.

  Workaround: There is no workaround.

- CSCue50101

  Symptom: ATM OAM packets are not being sent on the L2TPv3 tunnel when configured in transparent mode.

  Conditions: This symptom is observed when you enable oam-pvc manage on the CE.

  Workaround: There is no workaround.

- CSCue55739

  Symptom: PfR MC/BR session may be flapped, if PfR learn is configured with scale configuration.

  Conditions: This symptom may be observed, if PfR traffic-classes are learned by PfR global **learn** configuration.

  Workaround: Disable PfR global **learn** by configuring **traffic-class filter access-list** pointing to the **deny ip ip any** ACL, and configure PfR learn “list”.

- CSCue59592

  Symptom: Multiple crashes observed with the following tracebacks after upgrading the Cisco IOS Release from 12.2(33)SRC1 to 12.2(33)SRE6:

```
*Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to lock a
semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
9E19F1C 9E1D4FC
```

Conditions: The symptom is observed with a combination of BGP VPNv4 prefixes and PBR enabled on the interface for the VRF and during upgrade of image or reload of the device. If "mls mpls recirc agg" is enabled in global mode, then this crash will not be observed.

Workaround: Enable "mls mpls recirc agg" in global mode.

- CSCue61691

  Symptom: In a dual-homing topology, switching from the backup mode to the nominal mode ends up with the active "source" router sending a data MDT but transmitting on the default MDT.

  Conditions: The symptom is observed on a dual-homing topology with CORE GRE tunnel.

  Workaround: Use the following command:

  ```
  clear ip mroute vrf <>
  ```

- CSCue68761

  Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3. Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3.

  ```
  ------------------ show buffers ------------------
  Buffer elements: 156 in free list (500 max allowed) 11839912 hits, 0 misses, 617
  created
  Public buffer pools: Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @
  10:04:00): 0 in free list (20 min, 150 max allowed) 7968057 hits, 202704 misses, 2128
  trims, 47265 created 71869 failures (680277 no memory)
  ------------------ show buffers usage ------------------
  Statistics for the Small pool Input IDB : Mu1 count: 45180 Caller pc : 0x22CF95C4
  count: 45180 Resource User: IP Input count: 45180 Caller pc : 0x22381654 count: 2
  Resource User: Init count: 2 Output IDB : Mu1 count: 4 Caller pc : 0x2380114C count: 4
  Resource User: PIM regist count: 4 Number of Buffers used by packets generated by
  system: 45187 Number of Buffers used by incoming packets:
  ++++++++++++++++++++++++++++small buffer packet++++++++++++++++++++++++++++++++
  <snip>
  Buffer information for Small buffer at 0x2A815220 data_area 0xD9DEB04, refcount 1,
  next 0x0, flags 0x2080 linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1 if_input
  0x30F21520 (Multilink1), if_output 0x0 (None) inputtime 00:02:46.212 (elapsed
  05:55:11.464) outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
  datagramstart 0xD9DEB56, datagramsize 38, maximum size 260 mac_start 0xD9DEB56,
  addr_start 0x0, info_start 0xD9DEB58 network_start 0xD9DEB58, transport_start
  0xD9DEB6C, caller_pc 0x22CF0044
  source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11, TOS: 192 prot:
  17, source port 496, destination port 496
  0D9DEB56: 002145C0 002455F0 .!E@.$Up 0D9DEB5E: 00000B11 F14C0A83 7C21E000 012801F0
  ....qL..|!`..(.p 0D9DEB6E: 01F00010 82211200 00000000 000000 .p...!.........
  ```

  Workaround: There is no known workaround. Reboot frees up memory.

- CSCue7605

  Symptom: On a SIP 400 with gigeV2 SPA, when EVC is configured with "encap default", it is seen that sometimes the FUGU TCAM is not programmed with correct VVID for the EVC. This results in incoming traffic reaching the linecard with wrong VVID. This can impact traffic incoming on the EVC.

  Conditions: The symptom is observed with an "encap default" configuration under EVC, or removal and re-application of "encap default" under EVC.

  Workaround: There is no workaround.

- CSCue76251

  Symptom: A BFD session is created for tunnel-tp without any BFD configuration underneath it.

  Conditions: This symptom occurs only on bootup and when there is no BFD configuration underneath tunnel-tp.

  Workaround: There is no workaround.

- CSCue86147

  Symptom: E-OAM state is going down when LACP is going down.

  Conditions: 7600--------- ALU 72

  There are LACP and E-OAM running on both the routers.

  The behavior we observe is that the Cisco 7600 puts a member link into OPER DOWN state if LACP is not received on the port (on active mode). This OPER DOWN link state is propagated to all protocols including E-OAM.

  This is incorrect as E-OAM runs below LACP and hence E-OAM must be able to receive/transmit and has a protocol state of UP irrespective of LACP indication if its state machine indicates so.

  Workaround: There is no workaround.

- CSCue94653

  Symptom: When the port-security configured interface goes to blocking state (MST), the VLANs configured on the port go to not-forwarding state temporarily. The secure mac-addresses are not added back resulting in loss of traffic.

  Conditions: The symptom is observed when the port-security configured interface goes to blocking state.

  Workaround: Shut and no shut the port-security interface to re-add the mac-addresses.

- CSCuf09006

  Symptom: Upon doing a **clear ip bgp * soft out** or **graceful shutdown** on a PE, all VPNv4/v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.

  Conditions: This symptom is observed under the following conditions:

  1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. OS version must have “Enhanced Refresh” feature enabled.
  4. A **clear ip bgp * soft out** or **graceful shutdown** is executed on the PE.

  Workaround: Instead of doing **clear ip bgp * soft out**, do a route refresh individually towards all neighbors.

- CSCuf17009

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

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

  Workaround: There is no workaround.

- CSCuf20409

  Symptom: Netsync: Customer seeing clock in ql-failed state on one Cisco ASR 2RU model.

  Conditions: The issue seen when distributing stratum 1 clock source through its network.

  Workaround: There is no workaround.

- CSCuf30554

  Symptom: Traffic drops with scalable EoMPLS.

  Conditions: This symptom occurs when the MPLS label allocates 21 bit for the label with TE tunnel in the core.

  Workaround: There is no workaround.

- CSCuf30798

  Symptom: SIP 600 crashes.

  Conditions: The symptom is observed with VPLS VC going over GRE tunnel and chassis having both ES+ and SIP 600 card.

  Workaround: Remove VPLS over GRE. This configuration is not supported.

- CSCuf64313

  Symptom: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

- CSCuf81275

  Symptom: Some ISG sessions do not pass traffic.

  Conditions: This symptom is observed when you have more than one Line Card for the ISG sessions.

  Workaround: There is no workaround.

- CSCug17808

  Symptom: Redistributed default route not advertised to EIGRP peer.

  Conditions: This symptom is observed when Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command, the route disappears form the spokes.

  Workaround: Clearing the EIGRP Neighborship restores the route on the spokes.

- CSCug23348

  Symptom: The “mod” value in the SSRAM may be inconsistent to the number of ECMP paths.

  Conditions: This occurs with ECMP TE tunnels with **tunnel mpls traffic-eng load-share** *value* commands configured.

  Workaround: Remove the **tunnel mpls traffic-eng load-share** *value* commands from the TE tunnels.

- CSCug50208

  Symptom: A crash is seen due to double free of memory.

  Conditions: The symptom is seen when the accept interface VLAN goes down.

  Workaround: There is no workaround.

- CSCug56942

  Symptom: CUOM could not process “MOSCQEReachedMajorThreshold clear trap” from CUBE SP. For MOSCqe alert clear trap, CUBE should not sent “CurrentLevel Varbind” but should send “csbQOSAlertCurrentValue Varbind”.

  Conditions: This symptom is observed when CUBE SP generates clear trap for voice quality alerts.

  Workaround: The code fix is included in CUBE Cisco IOS Release 15.2(4)S4. Manually clean the alarm at CUOM after root cause is rectified if earlier CUBE version is used.

- CSCug58977

  Symptom: 2.6Gbp/s traffic is observed on both of the VPN SPA interfaces. Traffic direction: Rx on outside interface, Tx on inside interface.

  Conditions: Problem is triggered when fragmented IPSec packet arrives on clear side. Issue observed only in VRF mode.

  Workaround: Reload the IPSec card.

- CSCug68193

  Symptom: Multicast traffic across ES+ cards stop flowing across subinterfaces.

  Conditions: The symptom is observed after a linecard OIR. After the linecard comes up, multicast traffic stops flowing across subinterfaces.

  Workaround: Shut/no shut the subinterface.

- CSCug72891

  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.

  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.

  Workaround: There is no workaround.

- CSCug78098

  Symptom: Supervisor engine crashes and the Cisco IOS software is forced to reload due to PIM process.

  Conditions: This symptom is observed when using the command, **show ip pim rp-hash** right after the BSR RP times out, causes the crash.

  Workaround: Perform these steps in the following order:

  1. Wait for a minute after BSR RP times out before using this command.
  2. Configuring **no ip domain lookup** will make the time taken to execute **show ip pim rp-hash** to a few milliseconds. This will prevent the crash from being reproduced manually.

- CSCug94275

  Symptom: ES+ card crashes with an unexpected exception to CPU: vector 200, PC = 0x0.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCug98820

  Symptom: Multicast RP-Announcement/RP-Advertisement packet is replicated more than one copy per incoming packet. The number of copies is equal to the number of interfaces/IOitems with IC flag enabled (show ip mfib to get the number of IC interfaces).

  Conditions: This symptom is observed when AUTO-RP filter is configured on PIM interfaces.

  Workaround: There is no workaround.

- CSCuh07349

  Symptom: A Cisco 7600 Sup may crash due to SP memory corruption.

  Conditions: This issue is observed on an REP enabled router, which is part of an REP segment. The exact trigger for this issue is not clear.

  Workaround: There is no workaround.

- CSCuh07657

  Symptom: VRF Aggregate label is not re-originated after a directly connected CE facing interface (in VRF) is shut down.

  Conditions: This symptom occurs in an MPLS VPN set-up with Cisco 7600(PE) Router running on Cisco IOS Release 12.2(33)SRE4 with per VRF aggregation. For example:

  ```
  mpls label mode vrf TEST protocol all-afs per-vrf
  ```

  Workaround: Downgrade to Cisco IOS Release 12.2(33)SRE3 or earlier.

- CSCuh16927

  Symptom: Mac entries learned on a trunk link are flushed after removing VLANs.

  Conditions: The symptom is observed when some allowed VLANs are removed on a trunk link, all mac address entries learned on this link are flushed. This is issue is specific to extended VLAN IDs.

  Workaround: Executing ping to destination IP after removing VLANs will recover this condition.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help.

  For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message.

  In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string "NSF peer closed the session"

  For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session NSF peer closed the session May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down
  Instead of: May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME
  Down BFD adjacency down May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE: neighbor
  x.x.x.x IPv4 Unicast vpn vrf VRFNAME topology base removed from session BFD adjacency
  down
  ```

  Log messages associated for non-BFD triggers are not documented.

Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (eg: clear command) is in progress.

Affected configurations all include: router bgp ASN ... bgp graceful-restart ...

The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP's CPU requirements.

It is not possible to trigger this bug unless BGP graceful-restart is configured.

Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptom section, and then take manual steps to remedy this problem when it occurs.

On the problematic router, issue **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes.

The other option is to manually shutdown the outgoing interface which marks the routes as "inaccessible" and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

More Information: This bug affects all releases where CSCsk79641 or CSCtn58128 is integrated. Releases where neither of those fixes is integrated are not affected.

- CSCuh40275

  Symptom: SNMP occupies more than 90% of the CPU.

  Conditions: This symptom is observed when polling the cefFESelectionTable MIB.

  Workaround: Execute the following commands:

  ```
  snmp-server view cutdown iso included snmp-server view cutdown cefFESelectionEntry
  excluded snmp-server community public view cutdown ro snmp-server community private
  view cutdown rw
  ```

- CSCuh40617

  Symptom: Ping fails when "ncap dot1q" is configured on an FE SPA inserted in bay 1 of flexwan.

  Conditions: This symptom is observed when FE SPA is inserted in bay 1 of flexwan.

  Workaround: Move the SPA to bay 0 of flexwan.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

- CSCuh48840

  Symptom: Cisco Router crashes.

  Conditions: This symptom is observed under the following conditions:

  1. To re-create the issue:

a. Sup-bootdisk formatted and copied with big size file, like copy 7600 image file around 180M size.

b. Reload box, and during bootup try to write file to sup-bootdisk (SEA write sea_log.dat 32M bytes). Then the issue appear

2. When the issue seen, check the sea_log.dat always with 0 byte

3. No matter where (disk0 or bootdisk) to load image.

4. No matter sea log disk to sup-bootdisk or disk0:. reproduce the issue with "logg sys disk disk0:" config.

```
SEA is calling IFS API to create sea_log.dat, looks like IFS creating file hungs SP.
sea_log.c : sea_log_init_file() -> ifs_open() -> sea_zero_log() -> ifs_lseek() ->
ifs_write()
```

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)S5a

Resolved Caveats—Cisco IOS Release 15.1(3)S5a

Cisco IOS Release 15.1(3)S5a is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S5a but may be open in previous Cisco IOS releases.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

Resolved Caveats—Cisco IOS Release 15.1(3)S5

Cisco IOS Release 15.1(3)S5 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S5 but may be open in previous Cisco IOS releases.

- CSCsx46323

  Symptoms: When a span monitor source or destination is a port-channel that is automatically created by a service module, the monitor configuration will be discarded on reloads. Also, for a redundant system, restarting the standby will cause the standby to continually reset, until the monitor session source/destination using the PO is removed.

  Conditions: This symptom occurs when the configuration is “monitor session x source interface port-channel yyy”, where yyy is the port-channel that is automatically created by the service module.

  Workaround: Remove the monitor session created on internal port-channels of service modules before any redundant SUP reset or reload. A full system reload will also cause the monitor session to be discarded and will therefore prevent a continual reload cycle of the standby.

- CSCtc42734

  Symptoms: A communication failure may occur due to a stale next-hop.

  Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.

  Workaround: Reload the router.

- CSCtd54694

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

  Conditions: This symptom is a rare timing issue.

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

- CSCtg39957

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

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

  This advisory is available at the following link:

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

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCti51196

  Symptoms: SSH to any IPv6 link-local address connects to itself.

  Conditions: This symptom is observed when you configure SSH and try to connect to any link-local address using SSH.

  Workaround: There is no workaround.

- CSCtj89743

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

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

  Workaround: There is no workaround.

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

- CSCtn40771

  Symptoms: The process ACL Header in the **show memory allocating- process totals** command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the **show process memory** command output to appear to have a leak.

  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.

  Workaround: There is no workaround.

- CSCtn41225

  Symptoms: The IPC port disappears and error messages are displayed on the Cisco CMTS. On the Cisco c76000 platform, it causes a crash.

  Conditions: This symptom is observed while doing a quit operation using the **show ipc util** command.

  Workaround: Do not use the **show ipc util** command.

- CSCtn56097

  Symptoms: Auto mpls-lsp-monitor for pathecho fails.

  Conditions: Auto mpls-lsp-monitor feature does not work due to internal scheduling error.

  Workaround: There is no workaround.

- CSCtn84205

  Symptoms: Bidirectional multicast group traffic will be software switched on a Cisco 7600 Router.

  Conditions: This symptom is observed when there are around 20 + (A) accept interfaces on the router for the bidirectional multicast group.

  Workaround: There is no workaround.

- CSCto87436

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

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

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

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C CVE ID CVE-2012-5014 has been

assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr44299

  Symptoms: The following error message is displayed: Config Sync: Line-by-Line sync verifying failure.

  Conditions: This symptom is observed when you configure service-engine command line interfaces.

  Workaround: There is no workaround.

- CSCtr87413

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

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

  Workaround: Use **clear crypto sa**.

- CSCts03251

  Symptoms: A Cisco 2921 router running Cisco IOS Release 15.1(4)M with the "logging persistent" feature configured may crash.

  Conditions: This symptom is observed with the "logging persistent" feature.

  Workaround: Disable the "logging persistent" feature.

- CSCts20857

  Symptoms: This issue is actually a fix for CSCtj96916, which is the original issue

  Conditions: This symptom occurs when changing the card type from T3 to E3.

  Workaround: There is no workaround.

- CSCts44393

  Symptoms: A Cisco ASR 1000 crashes.

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

  Workaround: There is no workaround.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

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

  Workaround: There is no workaround.

- CSCtu14086

  *MVPN over GRE PIM vrf neighbor not up after SSO

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.

Workaround: There is no workaround.

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

  Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

  Workaround: There is no workaround.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtu42387

  Symptoms: Gigabit and 10 Gigabit Fiber link reporting threshold violation alarm in Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The "%SFF8472-3-THRESHOLD_VIOLATION: Gi0/11: Rx power high alarm" error message is seen on ports.

  Conditions: This symptom is observed on Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The messages are seen with the interface shut or no shut.

  ```
  SFF8472-3-THRESHOLD_VIOLATION Gi5/1: Rx power low alarm; Operating value:
  -28.5 dBm, Threshold value: -24.0 dBm
  ```

  Workaround: Fixing the fiber signal issue or disconnecting the fiber from the transceiver has been known to stop the messages.

- CSCtw50952

  Symptoms: A Cisco ASR series router crashes due to memory exhaustion after issuing the **clear ip ospf**. This symptom was not observed before issuing this command.

  ```
  ACC-CDC-NET-Pri#sh mem stat
                  Head    Total(b)     Used(b)     Free(b)   Lowest(b)
  Largest(b)
   Processor   30097008   1740862372   279628560   1461233812   1460477804
   1453167736
   lsmpi_io   97DD61D0     6295088     6294120         968         968
     968
  ```

  Conditions: This symptom is observed upon executing the **clear ip ospf** causing tunnel interfaces to flap.

  Workaround: There is no workaround.

- CSCtx01918

  Symptoms: On the hub if you configure IVRF for static crypto-map then, after an invalid-spi recovery, the new ISAKMP has an incorrect IVRF (global). IPsec phase II fails with a "proxy identities not supported" error message. The other related issues seen are:

  1. Initial contact not being sent when IKE SA is triggered by invalid-spi recovery.
  2. When quick mode is initiated, it picks the self-initiated IKE SA and hence the QM packet is dropped at the other end.

Conditions: The symptom is observed with a router running HSRP with VRF aware IPsec static crypto map. When you shutdown the active router's external interface, the IPsec tunnel failsover to the standby router. The standby router has an invalid-spi recovery configured. The invalid-spi recovery kicks but new ISAKMP has an incorrect IVRF and IPsec phase II fails.

Workaround: Manually clear SA at spoke site using **clear crypto sa**.

- CSCtx23014

  Symptoms: HSRP hellos cannot be sourced from certain IPs.

  Conditions: This symptom is observed when HSRP hellos cannot be sourced for an IP address with a standby IP address in the same subnet and both are configured in the global VRF. For example:

```
Router(config)#interface Ethernet0/0
Router(config-if)# ip address 192.168.68.13 255.255.252.0
Router(config-if)# standby 68 ip 192.168.70.1
Router(config-if)# standby 68 priority 120
Router(config-if)# standby 68 preempt
Router(config-if)# arp timeout 300
```

  Workaround: Use an IP from the subnet for the SVI interface in the same VRF.

- CSCtx36095

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

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx57154

  Symptoms: RP crashes and brings down the router.

  Conditions: This symptom is observed upon shut/no shut of an ES+ access interface configured with 5K EVC.

  Workaround: There is no workaround.

- CSCtx68100

  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.

  Conditions: The symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the **show version** CLI is executed.

  Workaround: There is no workaround.

- CSCty07558

  Symptoms: DHCPv6 packets are dropped on a Cisco 7600 switch. For example, they are not flooded.

  Conditions: This symptom is observed when there is no IPv6 address on an SVI or if l2 VLAN has SVI in shut state (default existence after a new ACL feature).

  Workaround: Two possible workarounds which essentially serve as the fix due to the limitations they impose:

  1. When working with a pure L2 VLAN, remove ttl rate limiter (selected as default rate limiter on Cisco7600, but not on other boxes) using "no mls rate-limit all ttl-failure". 2)
  2. If the design permits and TTL rate limiter is necessary, put a dummy IPv6 address on the SVI or simply configure IPv6 enable on the SVI.

- CSCty12312

  Symptoms: Multilink member links move to an up/down state and remain in this condition.

  Conditions: This symptom occurs after multilink traffic stops flowing.

  Workaround: Remove and restore the multilink configuration.

- CSCty59891

  Symptoms: On the node where shut/no shut is issued, traffic does not reach IPsec VSPA, which is supposed to get encrypted.

  Conditions: This symptom is observed when issuing shut/no shut on the GRE tunnel protected with IPsec and QoS configured on this IPsec tunnel.

  Workaround: Remove and attach “tunnel protection ipsec profile”.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: The symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: The symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty99846

  Symptoms: Cisco IOS software includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

  CVE-2009-1386

  This bug was opened to address the potential impact on this product.

  Conditions: This symptom occurs when device is configured with SSLVPN and **svc dtls**.

  Workaround: Disable DTSL with **no svc dtls**.

  Further Problem Description: This problem would only be seen in Cisco IOS when using Anyconnect client with Cisco IOS SSLVPNs, after the initial session has been authenticated and established. Exploitation would result in Cisco IOS reloading.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2009-1386 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

- CSCtz28023

  Symptoms: Traffic is not forwarded for a few mroutes.

  Conditions: This issue is seen when multiple routers in the network are reloaded simultaneously.

  Workaround: Using the **clear ip mroute vrf** *vrf name* command may resolve the issue.

- CSCtz34869

  Symptoms: Aps-channel stops working.

  Conditions: This symptom occurs with an open ring and is seen in the following scenario:

  ```
  A1(po2)(RPL)<=======>(po2)A3 (gig3/2)<=======>(gig3/3)A4
  ```

  Shut down gig3/2 on A3. Does not make A1 into protection.
  => Debugs show no SF packets are being transmitted to A1 which is connected to A3 via "Port-channel"
  => A1 (po2) is RPL of the ring. It is not going to unblocked even after A3-A4 link goes down.

  Workaround: Reload the line card.

- CSCtz39917

  Symptoms: The VC status for CE routers is inactive.

  Conditions: This symptom is observed when PE1 router reload.

  Workaround: There is no workaround.

- CSCtz43626

  Symptoms: Minor or major temperature alarms reported in the syslog:

  ```
  %C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.

  %C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: The symptom is observed on ES+ series line cards of Cisco 7600 series routers. Specifically, the reported temperature will be far off from reading of other sensors on the line card.

  Workaround: There is no workaround.

- CSCtz44989

  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of "XXXX" networks are removed.

  Workaround: The **show ip route XXXX** command (without "XXXX") does not have the problem.

- CSCtz65541

  Symptoms: The following error is encountered in Console logfile:

  ```
  %AAA-3-PARSEERR: Error(2) parser is unable to parse nono IP route vrf
  ```

Conditions: This symptom is observed when large number of L2TP sessions with Radius defined VRF routes are cleared or disconnected.

Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

```
CE0------------------PE0--------------------RR
                         |                      |
                         |                      |
CE1------------------PE1----------------------|
```

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

  This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

  Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

  Workaround: Hard clear.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is seen when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCtz88879

  Symptoms: When testing for DMVPN in a HUB-SPOKE topology, where there are 170 tunnels protected with IPsec on Spoke and one mGRE tunnel on hub. B2B redundancy is configured. No QoS is applied on the scaled IPSec tunnels. Upon doing SSO with this configuration, the a "%VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnelx: allocated idb has invalid vlan id" error message is seen repeatedly on the new active and the router becomes almost inaccessible. As can be seen from **show vlan int usage** command output, there are more than 3K free VLANs on both the Hub and Spoke.

```
*May 14 12:31:10.315: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel87: allocated idb has
invalid vlan id
*May 14 12:31:10.511: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel26: allocated idb has
invalid vlan id
*May 14 12:31:10.543: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel28: allocated idb has
invalid vlan id
*May 14 12:31:10.575: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel90: allocated idb has
invalid vlan id
```

After a continuous flood of error messages, a Granikos crash is seen, and the **show cry eli** command shows only one SPA and this SPA is stuck in INIT state.

Conditions: This symptom occurs when doing a shut/no shut using the **interface range** command, and once all tunnels are up, doing an SSO.

Workaround: There is no workaround.

- CSCtz94902

  Symptoms: Memory allocation failure occurs when attaching to SIP-40 using a web browser.

  Conditions: This symptom occurs on the line card.

  Workaround: Reset the line card.

- CSCtz95756

  Symptoms: The "%INTR_MGR-3-INTR: SIP1/3: SPA ATM1/3 FPGA PCI FIFO" message is seen on 6RU.

  Conditions: This symptom is observed when reloading the PE2 router.

  Workaround: There is no workaround.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

```
RADIUS:  Acct-Session-Id     [44]  10  "00000001"
RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
        [7]
RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0

 RADIUS:  Acct-Delay-Time     [41]  6   0
```

  Conditions: Occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua07927

  Symptoms: MLDP traffic is dropped for local receivers on a bud node.

  Conditions: This issue is seen on doing stateful switchover (SSO) on bud node.

  Workaround: Using the **clear ip mroute vrf** *vrf name* ***** command for the effected VRFs will resume the MLDP traffic.

- CSCua12396

  Symptoms: IPv6 multicast routing is broken when we have master switchover scenarios with a large number of members in stack. Issue is seen on platforms like Cisco 3750E and Cisco 3750X where IPV6 multicast routing is supported.

Conditions: This symptom is observed when IPV6 multicast routing is configured, mcast routes are populated and traffic is being forwarded. Now, in case of master switchover, synchronization between master and members is disrupted. This is seen only for IPv6 multicast routing. Observed the issue with 9-member stack and either during first or second master switchover. No issues are seen for IPv4 multicast routing.

Workaround: Tested with 5-member stack, and no issues are seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in stack.

- CSCua13848

  Symptoms: The Cisco ASR 1000 crashes.

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

  Workaround: There is no workaround.

- CSCua20373

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

  Conditions: This symptom is observed when Vanilla GRE tunnels are configured in the system where HA and the IPsec Module SSC-600/WS-IPSEC-3 card is present, “crypto engine mode vrf” is configured and SSO is issued.

  Workaround: Remove the “crypto engine mode vrf” configuration if IPsec is not enabled on the router.

- CSCua25671

  Symptoms: After adding the source interface in RSPAN, there is huge flooding to all trunks allowing RSPAN VLAN starts, even if there is no traffic on the RSPAN source interface.

  Conditions: This symptom is observed under the following conditions:

  1. The router has a RSPAN source session.
  2. The source interface being added to the RSPAN source session is on ES+.
  3. Any of the ES+ modules in the system has an interface on the RSPAN VLAN (that is, at least one of the interfaces on an ES+ module carries RSPAN replicated traffic).
  4. The online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, are enabled on the ES+ module which has 2 and 3 mentioned above.

  Workaround 1: Disable the online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, on the ES+ module which has the RSPAN source.

  Workaround 2: If you have to use an interface on the ES+ module as a SPAN source, make sure that no other interface on any of the ES+ modules in the system is in the RSPAN VLAN. If you have to use an interface on the ES+ module to carry RSPAN replicated traffic, make sure that no other interface on any of the ES+ modules in the system is being monitored as an RSPAN source.

- CSCua25943

  Symptoms: CPU Hog is observed on the LC when the number of IPv6 prefixes pumped in is more than 10,000.

  Conditions: This symptom is observed when more than 10,000 IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua26064

  Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

  Conditions: This symptom is seen when there are 4 core facing tunnels that load balance traffic to these prefixes. The **show mls cef ipv6** *prefix* **detail** command shows the different adjacencies taken by different prefixes.

  Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

  Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

  Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations.

  ```
  snmp-server view view name iso included
  snmp-server view view name ceeSubInterfaceTable excluded
  snmp-server community community view view name nterfaceTable excluded
  snmp-server community community view view name
  ```

- CSCua29095

  Symptoms: Spurious memory access is seen when booting the image on a Cisco 7600 router.

  Conditions: This symptom occurs while booting the image.

  Workaround: There is no workaround.

- CSCua31157

  Symptoms: One way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.

  Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly one minute after the tunnel between the spokes came up.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCua40273

  Symptoms: The Cisco ASR 1000 crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the Cisco ASR 1000 with Cisco IOS Release 15.1(2)S.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua47570

  Symptoms: The **show ospfv3 event** command can crash the router.

  Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.

  Workaround: Do not use the **show ospfv3 event** command.

- CSCua52289

  Symptoms: CPU hog is seen on the line card due to Const2 IPv6 process.

  Conditions: This symptom occurs with 4 core facing tunnels. Upon FRR cutover, the CPU hog is observed.

  Workaround: There is no workaround.

- CSCua56999

  Symptoms: Abnormal line card reload occurs.

  Conditions: This symptom occurs when an MVPNv6 scaled router acts as PE on which source traffic is ingressing and the line card is connected on the access side.

  Workaround: There is no workaround.

- CSCua57585

  Symptoms: CPU utilization increases with XE3.3 builds.

  Conditions: Occurs when a device forwards traffic on PPPoE connections.

  Workaround: There is no workaround.

- CSCua57728

  Symptoms: Traffic loss of ~25s is seen upon doing TE FRR Cutover with IPv6 prefixes.

  Conditions: This symptom is observed with four core facing tunnels, and 100,000 IPv6 prefixes. Shut the primary interface and check for the traffic loss.

  Workaround: There is no workaround.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if,

  1. BGP graceful restart is enabled.
  2. The next-hop is learned by BGP.

  Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCua67532

  Symptoms: IPsec sessions fail to come up.

  Conditions: This symptom occurs when Site-Site crypto configuration using crypto map is applied on SVI, and when no ISAKMP profile is configured under that crypto map.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

Workaround: There is no workaround.

- CSCua68243

  Symptoms: IGMP and PIM control packets are not reaching RP. As a result, the mac-address table for IGMP snooping entries is not populated.

  Conditions: This can be seen on a Cisco 7600 series router that is running Cisco IOS where IGMP and PIM control packets come in on an SVI only after the condition where the SVI link state goes down and comes up again. This does not affect routed ports.

  Workaround: In the SVI configuration mode:

  1. Unconfigure PIM by using **no ip pim**.
  2. Unconfigure IGMP snooping by using **no ip igmp snooping**.
  3. Re-enable both PIM and IGMP snooping.

- CSCua68398

  Symptoms: The ES+ card crashes.

  Conditions: This symptom is observed with a scaled EVC and VPLS configurations.

  Workaround: Stop the traffic. After the line cards boot up and the ports are up, start the traffic.

- CSCua75069

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

  Conditions: This symptom is observed only when all of the following conditions are met:

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

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

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

  Older releases on these trains are not impacted.

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

- CSCua85239

  Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller “mtu” or “ip mtu” configured.

```
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP Notification sent
%BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0 (hold time expired) 0 bytes
%BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4 Unicast topology base removed from
session BGP Notification sent
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to 2.2.2.5(17744) tableid - 0
```

  Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

  - f the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will be force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
  - Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

  Workaround: There is no workaround.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua90061

  Symptoms: The WS-IPSEC-3 Module crashes post configuration change.

  Conditions: This symptom occurs when you dynamically modify the GRE tunnel protected with IPsec to the sVTI tunnel and vice versa while traffic is traversing across the IPsec tunnel.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCua99035

  Symptoms: When enabling the “mls mpls tunnel-recir”, the Tunnel Reserved VLAN 6RD tunnel is allocated. If there is a Tunnel Reserved VLAN, then an extra VPN is allocated. VPN space will be exceeded when you scale up the 6RD tunnel, and you will notice VPNMAP-SP-2-SPACE_EXCEEDED messages. You can verify the output of the VPN table.

```
RTHS_UUT_PE1-sp#sh platform software vpn status
Errors:
```

```
 Exceeded Space: 998  ----------------------------------------> exceeded the
VPN Space
Entries reserved for 6VPE:  255
Entries used by 6VPE:       255 ---------------------------------> We have 253
IPv6 VRF, but it is showing more than configured VRF.
Entries free on 6VPE:       0
Entries used by no-v6 VRFs: 500
Entries used by MLS applic: 3
Entries free for all no-v6: 3337
```

Conditions: This symptom is observed under the following conditions:

1. Configure the ""“mls mpls tunnel-recir” on the router along with the 6RD Tunnel configuration.
2. When you insert ES-20 into the existing system, “mls mpls tunnel-recir” will be configured by default.

Workaround: There is no workaround.

- CSCua99969

  Symptoms: IPv6 PIM null-register is not sent in the VRF context.

  Conditions: This symptom occurs in the VRF context.

  Workaround: There is no workaround.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. “Volume rekey” is disabled on Zamboni.

  Conditions: This symptom occurs if we have “volume rekey” disabled on Zamboni.

  Workaround: Do not disable the volume rekey on Zamboni.

- CSCub07855

  Symptoms: The VRF error message is displayed in the router.

  Conditions: This symptom occurs upon router bootup.

  Workaround: There is no workaround.

- CSCub10951

  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

  Conditions: This symptom is observed with the following conditions:

  1. The following configuration exists at all RRs that are fully meshed:
  – bgp additional-paths select best-external
  – nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is,
  – Overall best path via RR1.
  – Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.
  – Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.

3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
4. At PE6, reconfigure the route so that RR5 will have "ic_path_rr5" as its "best-external (internal) path". At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

Workaround: Hard/soft clear.

- CSCub21468

  Symptoms: UDP header is corrupted randomly.

  Conditions: This symptom is observed with the Cisco 7609-S (RSP720-3C-GE) running Cisco IOS Release 12.2(33)SRE5, with the VRF Aware LI feature.

  Workaround: There is no workaround.

- CSCub23231

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

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

  Workaround: Reload LC.

- CSCub31902

  Symptoms: Alignment correction tracebacks are seen from within the diag_dump_lc_l2_table() cosmetic issue, which create temporary memory inconsistencies in the function.

  Conditions: This symptom occurs in normal conditions, during bootup time, provided testMacNotification fails.

  Workaround: Disable bootup diagnostics or disable the testMacNotification health monitoring test.

- CSCub36356

  Symptoms: Scaling up routes result in huge memory allocations, eventually depleting the SP memory, leading to MALLOC FAIL and subsequent system crash.

  Conditions: This symptom occurs in normal conditions.

  Workaround: There is no workaround.

- CSCub36376

  Symptoms: Traffic is seen to be sent out of the bridging subinterface even when it is in the shutdown state. This issue is seen on the SPA Gigabit Ethernet interface. The issue occurs on all V2 Gigabit Ethernet SPAs.

  Conditions: This symptom is observed when the Gigabit Ethernet interface on the SPA sends traffic even in shutdown state.

  Workaround: There is no workaround.

- CSCub39268

  Symptoms: Cisco ASR 1000 devices running an affected version of IOS-XE are vulnerable to a denial of service vulnerability due to the improper handling of malformed IKEv2 packets. An authenticated, remote attacker with a valid VPN connection could trigger this issue resulting in a reload of the device. Devices configured with redundant Route Processors may remain active as long as the attack is not repeated before the affected Route Processor comes back online.

  Conditions: Cisco ASR1000 devices configured to perform IPSec VPN connectivity and running an affected version of Cisco IOS-XE are affected. Only authenticated IKEv2 connection is susceptible to this vulnerability.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-5017 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCub39296

  Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

  Conditions: The symptom is observed on the ES+ series line cards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCub47520

  Symptoms: "Match dscp default" matches router initiated ARP packets.

  Conditions: This issue seen on Cisco 7600 ES+ line cards.

  Workaround: Classify router generated packets using source mac address using a MAC ACL.

- CSCub48120

  Symptoms: Sp crash is observed @oce_to_sw_obj_type on a router reload.

  Conditions: This symptom is seen with core link flap at remote end during IP- FRR cutover.

  Workaround: There is no workaround.

- CSCub48262

  Symptoms: The router crashes in ROMmon.

  Conditions: This symptom occurs in RSP.

  Workaround: There is no workaround.

- CSCub53398

  Symptoms: The router crashes on bootup.

  Conditions: This symptom occurs when the router is booted up with a scaled MVPNv6 configuration. This issue is highly dependent on the "back walk" timing and sequence; hence, the probability to encounter the issue is low.

  Workaround: Disable power to all DFC modules on reload and bring them up one by one post reload.

- CSCub54261

  Symptoms: In an MLDP + MVPNv6 setup, abnormal RP reload occurs after the deletion and addition of few subinterfaces on the encapsulated PE.

  Conditions: This symptom occurs after deletion and addition of few subinterfaces on the router acting as the encapsulated PE on the access side for a few VRFs running MLCP inband.

  Workaround: There is no workaround.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

Workaround: Use a shorter prefix.

Further Problem Description: This issue does not affect software switching platforms.

- CSCub58312

  Symptoms: When IGMP query with source IP address 0.0.0.0 is received on an interface, it is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  IGMP querying router is 0.0.0.0 <----

Router#sh ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Po1,Po8,Router<-----
```

  Conditions: This symptom is seen when IGMP query with source IP address 0.0.0.0 is received.

  Workaround: There is no workaround.

- CSCub70336

  Symptoms: The router can crash when “clear ip bgp *” is done in a large-scale scenario.

  Conditions: This symptom is observed only in a large-scale scenario, with ten of thousands of peers and several VPNv4/v6 prefixes.

  Workaround: “clear ip bgp *” is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.

- CSCub73787

  Symptoms: The RSP720 may crash if a high rate of traffic is punted to the RP.

  Conditions: This symptom occurs on a Cisco 7600 with RSP720. It is specific to a driver used only by the RSP720. Other supervisor models are not affected. The issue is only seen in Cisco IOS Release 15.1(03)S and later releases, because of a code change made to the RSP720 driver.

  Workaround: Isolate and stop the traffic being punted to the RP.

- CSCub78830

  Symptoms: Traffic matching WCCP service gets black-holed.

  Conditions: This symptom is observed in vrf-wccp scenario and on redirection into MPLS cloud using GRE encap.

  Workaround: There is no workaround.

- CSCub79035

  Symptoms: Multicast traffic will get route cached on the receiver/decap node resulting in traffic drop and slight increase in RP/SP CPU.

  Conditions: This symptom is seen when multicast traffic flowing over GRE tunnel protected with IPsec and PIM is enabled on the GRE tunnel.

  Workaround: There is no workaround.

- CSCub86706

  Symptoms: After multiple RP switchover, the router crashes with the "UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO" error.

  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.

  Workaround: There is no workaround.

- CSCub87579

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

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

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

- CSCub89711

  Symptoms: The **atm** keyword for the **show** command disappears.

  Conditions: This symptom occurs when you do a powered shutdown of the SPA card and bring it back up using the **no** form of the previous command.

  Workaround: There is no workaround.

- CSCub91428

  Symptoms: Internal VLAN is not deleted even after waiting for 20 minutes, and the VLAN cannot be reused.

  Conditions: This symptom is seen with any internal VLAN allocated dynamically that is not freed up after 20 minutes in the pending queue.

  Workaround: There is no workaround.

- CSCub91546

  Symptoms: Traffic is dropped silently on the VLAN.

  Conditions: This symptom is observed when all the VLANs in the router are used (0 free VLAN). Any new internal VLAN creation will fail, and an appropriate error message is not shown.

  Workaround: There is no workaround.

- CSCub91815

  Symptoms: Certificate validation fails with a valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCub98140

  Symptoms: The router crashes at pak_subblock_share. CDETS commit is a cause for this issue. It is not a part of the released code.

  Conditions: This symptom occurs at pak_subblock_share. This issue is not a part of the released code.

  Workaround: There is no workaround.

- CSCub98588

  Symptoms: The IPsec session does not come up for spa-ipsec-2g if you have disabled "Volume Rekey".

Conditions: This symptom occurs when “Volume Rekey” is disabled on spa-ipsec-2g.

Workaround: Do not disable the “Volume Rekey” on spa-ipsec-2g.

- CSCuc06024

  Symptoms: Traffic flowing through EVCs that do not belong to any service group will see incorrect bandwidth values because of wrong bandwidth value programmed on the port-default node.

  Conditions: This symptom is seen when a mixture of flat and HQoS SGs having bandwidth configurations on their policies are applied on PC EVCs. Two mem- links are part of this PC, and default load-balancing is used.

  Workaround: There is no workaround.

- CSCuc10586

  Symptoms: In the Cisco 7600, multicast traffic does not flow in some scenarios. In the case of PIM SM mode, many times, (*,G) is present, but not (S,G) in mroute. In the case of PIM SSM mode, (S,G) is present but still traffic does not flow through.

  Conditions: This symptom is observed only with Cisco IOS Release 15S-based releases.

  Workaround:

  – Either use a different source IP or a different group IP.
  – Reload the module.

- CSCuc15810

  Symptoms: MVPN over GRE PIM VRF neighbor is not up after SSO.

  Conditions: This symptom is seen when MVPN over GRE PIM VRF neighbor is not up after SSO.

  Workaround: There is no workaround.

- CSCuc19046

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

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

  Workaround: There is no workaround.

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

- CSCuc28757

  Symptoms: IPv6 HbH Traffic traversing across BD SVIs will not be rate-limited by HbH rate-limiter that is configured.

  Conditions: This symptom is seen when enabling HbH rate-limiter on an NP of ES+ and IPv6 HbH traffic traversing across SVIs part of EVC BD of ES+ interface.

  Workaround: There is no workaround.

- CSCuc29884

  Symptoms: Outage and CPU remain astonishingly high against XDR MCAST process on a scaled HWO BFD testbed.

  Conditions: This symptom is seen after a router reload, when OSPF converge is getting completed, and started 10g traffic through the box.

  Workaround: There is no workaround.

- CSCuc32119

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

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

  Workaround: There is no workaround.

- CSCuc35935

  Symptoms: Traffic coming in with a particular label might experience drops on ES+.

  Conditions: This symptom is observed with traffic coming in on the ES+ interface with MPLS enabled. This issue is seen when the box has AToM (Scalable mode on the Cisco 7600) configured.

  Workaround: Reset the core facing ES+ module.

- CSCuc38851

  Symptoms: DHCP snooped bindings are not restored after an RTR reload.

  Conditions: This symptom might occur when bindings are learnt on Cisco ES20 EVCs.

  Workaround: After the RTR is UP, renew from the agent database by issuing the **renew ip dhcp snooping database** *URL* command.

- CSCuc41369

  Symptoms: Complete traffic loss occurs for V6 mroutes.

  Conditions: This symptom occurs during deletion and addition of VRFs for the MVPNv6 inband signaling configuration.

  Workaround: There is no workaround.

- CSCuc46356

  Symptoms: Router hangs and crashes by WDOG.

  Conditions: This symptom occurs when IPv6 ACL is applied to a port-ch sub-if. The sub-if is deleted followed by deletion of the ACL.

  Workaround: Delete the ACL before deleting the port-ch sub-if.

- CSCuc48162

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

  Conditions: This symptom occurs when EFP is admin down.

  Workaround: There is no workaround.

- CSCuc55346

  Symptoms: SNMP MIB cbQosCMDropPkt and cbQosCMDropByte report 0.

  Conditions: This symptom is observed with Cisco IOS Release15.1(3)S1 and Cisco IOS Release 15.2.This issue is not seen with Cisco IOS Release 12.2(33)SRE4.

  Workaround: Use SNMP MIB cbQosPoliceExceededPkt and cbQosPoliceExceededByte.

- CSCuc60245

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

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

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

- CSCuc65424

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

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

  Workaround: Turn off the IDB reuse option.

- CSCuc72244

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

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

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

  Workaround: There is no workaround.

- CSCuc90011

  Symptoms: Memory leak is caused by executing “show vpdn history failure” after PPP authentication failure.

  Conditions: This symptom occurs when executing the “show vpdn history failure” CLI.

  Workaround: There is no workaround.

- CSCuc96345

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

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

  14-73-73

  20-73-55

  4C-73-67

  4C-73-A5

  54-73-98

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

  64-73-E2

  70-73-CB

  8C-73-6E

  98-73-C4

  A0-73-32

  C4-73-1E

  D0-73-8E

  F0-73-AE

F4-73-CA

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

Sample configuration:

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

Workaround:

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

- CSCuc97711

  Symptoms: After SSO, traffic on the P2P-GRE tunnel within an MVPN may be affected.

  Conditions: This symptom is observed with Cisco IOS Release SREx- and RLSx-based releases.

  Workaround: Shut/no shut the P2P tunnel interface.

- CSCud03273

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

  Conditions: This symptom occurs under the following conditions:

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

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

- CSCud07856

  Symptoms: SP crashes at "cfib_update_ipfrr_lbl_ref_count".

  Conditions: This symptom is observed with a scaled IP-FRR configuration.

  Workaround: Remove the IP-FRR configuration.

- CSCud17934

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

Conditions: This symptom is observed with the following conditions:

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

Workaround: Use another HW on the MPLS core.

- CSCud19230

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

```
%PM_SCP-SP-1-LCP_FW_ERR: System resetting module 2 to recover from error:
x40g_iofpga_interrupt_handler: LINKFPGA IOFPGA IO Bus Err val: 4214784 Bus
Error Add:332 Bus Err
data: 0

%OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled Off (Module Reset
due to exception or
user request)

%C7600_PWR-SP-4-DISABLED: power to module in slot 2 set Off (Module Reset due
to exception or user
request)
```

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

  Workaround: There is no workaround.

- CSCud19257

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

  Conditions: This symptom is observed with a NAT configuration.

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

- CSCud27379

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

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

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

- CSCud28759

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

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

  Workaround: There is no workaround.

- CSCud33564

  Symptoms: BFD sessions are not offloaded.

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

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

Workaround: Reload ES+ cards.

- CSCud36208

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

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

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

Resolved Caveats—Cisco IOS Release 15.1(3)S4

Cisco IOS Release 15.1(3)S4 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S4 but may be open in previous Cisco IOS releases.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCtj93356

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

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

  Workaround: There is no workaround.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- CSCto02712

  Symptoms: A router that is running Cisco IOS Release 15.1(4)M1 with “proxy- arp” enabled will incorrectly reply to duplicate address detection ARP requests sourced from end devices.

  Some end devices will send an ARP request for their assigned IP to check for duplicate address detection per RFC5227. When this occurs the router should ignore this ARP request. With this issue, the router will respond to the request, which triggers the duplicate address detection on the end device and breaks connectivity between the router and end device.

  Conditions: The symptom is observed with the following conditions:

  – “Proxy-arp” is enabled on client facing Layer-3 interface.

  – End device sends a “duplicate address detection” ARP request on its local subnet.

  Workaround 1: Configure **no ip proxy arp** on client-facing interface.

  Workaround 2: Disable “duplicate address detection” on the end device.

- CSCto16377

  Symptoms: DPD deletes only IPSec SA and not IKE SA.

  Conditions: This symptom is observed when DPD is enabled and peer is down.

  Workaround: Manually delete the stuck ISAKMP session by using the **clear crypto isakmp conn-id** command. You can get the conn-id from the **show crypto isakmp sa** command output.

- CSCto85731

  Symptoms: Crash seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: The symptom is observed under the following conditions:

  1. Configure hub and spokes (flexvpn-nhrp-auto connect) as given in the enclosure.
  2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
  3. Do a **clear crypto session** at Spoke1.
  4. Repeat steps 2 and 3 a couple of times.

  Workaround: There is no workaround.

  Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to- spoke channel. The crash decode points to “nhrp_cache_info_disseminate_internal” function

- CSCtq99664

  Symptoms: Traffic does not egress from the interface.

  Conditions: The VRF set on the interface is originally configured for IPv4 and IPv6 address family. If the VRF is reconfigured to remove the IPv4 address family, then all interfaces in that VRF stop sending traffic.

  Workaround: Shut down and re-enable the interface in question.

- CSCtr61623

  Symptoms: The RP crashes at _be_ace_create_acl_node.

  Conditions: This symptom is observed when configuring the 4K DVTI VT.

  Workaround: There is no workaround.

- CSCts12499

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

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

  Workaround: There is no workaround.

- CSCts16569

  Symptoms: The router might reload unexpectedly with scaled serial interfaces configuration.

  Conditions: This symptom occurs during scaling to 4000 NSR peers with 1.5M routes.

  Workaround: There is no workaround.

- CSCts27674

  Symptoms: The static route is not injected to the routing table after enabling crypto map on the interface.

  Conditions: This symptom occurs when you configure “reverse-route static” in the crypto map.

  Workaround: Reconfigure “reverse-route static”.

- CSCts56044

  Symptoms: A Cisco router crashes while executing a complex command. For example:

  ```
  show flow monitor access_v4_in cache aggregate
  ipv4 precedence sort highest ipv4 precedence top 1000
  ```

  Conditions: This symptom is observed while executing the **show flow monitor top** top-talkers command.

  Workaround: Do not execute complex flow monitor top-talkers commands.

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts83046

  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.

  Conditions: The symptom is observed when HWIDB is removed from the list (through **list remove**) before it gets dequeued.

  Workaround: There is no workaround.

- CSCts84132

  Symptoms: Kingpin crashes.

  Conditions: This symptom is occurs during reload with a 4096 subinterface.

  Workaround: Disable CDP.

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

Workaround: There is no workaround.

- CSCtt43552

  Symptoms: A Cisco router reloads with the **warm-reboot** command.

  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.

  Workaround: There is no workaround. Remove CLI “warm-reboot” from configuration (router will not be able to use warm reboot feature).

- CSCtt99627

  Symptoms: The **lacp rate** and **lacp port priority** commands may disappear following a switchover from active to standby RP.

  Conditions: This affects the Cisco 7600 platform.

  Before performing a switchover one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP then they will disappear if a switchover occurs.

  Workaround: Prior to switchover if the commands do not show up on the standby RP as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue.

  Otherwise if the commands disappear after a switchover then the commands must be reconfigured on the newly active RP.

- CSCtu01601

  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.

  Conditions: This issue may be triggered when the memory in the router is low.

  Workaround: There is no workaround.

- CSCtu23195

  Symptoms: SNMP ifIndex for serial interfaces (PA -4T/8T) becomes inactive after PA OIR.

  Conditions: The symptom is observed with a PA OIR.

  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: The symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.

  Workaround: Ensure all your PPP connections stay stable.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This issue is seen in the Cisco 7600 router with 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

Workaround: There is no workaround.

- CSCtw55401

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

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

  Workaround: There is no workaround.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

  Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

  ```
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
  ```

  Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw70298

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

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

  Workaround: There is no workaround.

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: “no shut” interface in QMOVESTUCK error message, remove QoS policies on interface & sub-interfaces, remove interface from T1/T3 controller; then rebuild configuration.

- CSCtw88599

  Symptoms: If “port acl” is configured, diagnostics for the port fail during bootup. If the port ACL is on a supervisor port then the router goes for a reload.

  Conditions: The symptom is observed when you configure “port acl” on a switch port and reload the router.

  Workaround: Disable diagnostics for the module.

  This issue will effect only if there is a switchport configured on the router. The issue will not affect the traffic or the filtering based on the ACL, even if the testAclDeny fails and the card is on MajFail (due to this test only).

  As a workaround, we can remove the switchport configs for the ports (if they exist), then give a reload and apply the configs after the router has come up. Alternatively, we can do a “no diagn crash” and try to bring up the router.

In case the router reloads, the ports will not go into shutdown state. Hence, it is a cosmetic issue. It can be ignored. If reloaded in presence of the switchport configs, it should come up after two reloads into minor error state.

- CSCtw98200

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

  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.

  RIP is configured with the **timers basic** *5 20 20 25* command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise** *5* command. These interfaces include the loopback and virtual-template interfaces too.

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

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

- CSCtw99991

  Symptoms: Chunk memory leak is seen in the ES+ LC after configuring the IP source guard EVC configurations.

  Conditions: This issue is seen on a Cisco 7600 router with ES+ LC running Cisco IOS interim Release 15.2(1.16)S.

  Workaround: There is no workaround.

- CSCtx04709

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.

  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The **clear ip eigrp topology** *network mask* command may remove unexpected active entry.

- CSCtx11598

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

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

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

  - none
  - standby reset
  - down

  This failure leads to unexpected system reload.

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

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

- CSCtx19332

  Symptoms: A Cisco router crashes when “remote mep” is unlearned while auto EOAM operations are executing.

  Conditions: This symptom is observed if “remote mep” is unlearned from the auto database (shutdown on interface or remote mep reload) while the “IP SLA ethernet-monitor jitter” operation is still running. The crash occurs if the initial control message times out.

  Workaround: There is no workaround.

- CSCtx32329

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.

  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the **show** command.

- CSCtx42751

  Symptoms: The following error message is displayed:

  ```
  %TRANSCEIVER-3-INIT_FAILURE: SIP2/0: Detected for transceiver module in
  TenGigabitEthernet2/0/0, module disabled
   %LINK-3-UPDOWN: SIP2/0: Interface TenGigabitEthernet2/0/0, changed state to down
  ```

  Conditions: This symptom is observed with the XFP-10GLR-OC192SR transceiver.

  Workaround: Configure “service unsupported-transceiver”.

- CSCtx45373

  Symptoms: Under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command, the “VRF specified does not match this router” error message is displayed. When you issue the **redistribute eigrp 1** command, it gets NVGENd without AS number.

  Conditions: This symptom occurs under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command.

  Workaround: Instead of using the **exit-af-interface** command to exit, if you give a parent mode command to exit, the issue is not seen.

- CSCtx48473

  Symptoms: A router crashes when the following command is executed:

  sh platform software xconnect circuit-index interface *tunnel-name* | **i** *VC- number*

  No crashinfo is generated on the RP and SP. Please see the attached console before the crash.

  Conditions: The above command must be executed.

  Workaround: There is no workaround.

- CSCtx59669

  Symptoms: Spikes are observed in UDP jitter RTT values for MPLS VPN based operations.

Conditions: This symptom is seen on a Cisco 7600 series router when there are a large number of packets configured per UDP operation. Some packets (~1%) exhibit large RTT delays. This is especially noticeable when BGP is exchanging a large number of routes.

Workaround: There is no workaround.

- CSCtx62138

  Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.

  Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.

  Workaround: There is no workaround.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- CSCtx66804

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: The symptom is observed with the following conditions:

  - “ppp lcp delay 0” is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx74051

  Symptoms: When doing an ISSU downgrade, IPv6 Flexible Netflow monitors may be displayed and running config shown with incorrect sub-traffic types.

  Conditions: This symptom happens on a downgrade to Cisco IOS Release 15.2(1)S (XE3.5). The monitors affected are those applied to IPv6. For example CLI like the following:

  ```
  interface fa0/0/0
    ipv6 flow monitor monitor-name input
  ```

  Workaround: Netflow code should still capture packets as expected on Cisco IOS Release15.2(1)S. However do a reboot of the device should be done before saving the running config, as the affected config saved will be incorrect and so will then fail to work on start-up.

- CSCtx74342

  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.

  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

  Workaround: Configuring SPF throttle timer can change the interval.

  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Routershow ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
     via Ethernet0/0, directly connected
```

- CSCtx77501

  Symptoms: Traffic is dropped at decap side of PE box.

  Conditions: This symptom occurs with SSO at decap side of MVPN set-up, DFC core-facing, 6748 access facing.

  Workaround: Do a switchover.

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when Enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx85247

  Symptoms: An ES20 line card is reset on doing redundancy switchover of RSPs.

  Conditions: This symptom is seen with redundancy switchover of RSPs.

  Workaround: There is no workaround.

- CSCtx89260

  Symptoms: Re-adding the deleted port channel interface is not initializing the snmp-index.

  Conditions: The symptom is observed when re-adding the deleted port channel interface.

  Workaround: Reloading the standby and then doing an RP switchover or doing a double RP switchover corrects the configuration.

- CSCtx94279

  Symptoms: A line card crashes.

  Conditions: This symptom is observed in switch traffic and flood traffic (line rate and less that 128-byte packet size) with more than one port in the egress path flood.

  Workaround: There is no workaround.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

Conditions: This symptom occurs when the IPv4 default route exists, that is:

```
ip route 0.0.0.0 0.0.0.0 <next-hop>.
```

Or a certain static/IGP route exists: For example:

```
ip route 0.0.253.0 255.255.255.0 <next-hop>.
```

Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

```
router bgp 65000
  address-family l2vpn vpls
   neighbor 10.10.10.10 next-hop-self
```

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty05150

  Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.

  Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.

  Workaround: Remove and reconfigure “area x stub”.

- CSCty06191

  Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a line card.

  Conditions: The symptom is observed with a multilink interface flap.

  Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.

- CSCty06990

  Symptoms: Intercepted packets are not forwarded to MD.

  Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.

  Workaround: Remove and reapply TAP.

- CSCty13647

  Symptoms: Symptoms vary from one image to another. The following symptoms have been mostly observed:

  1. Spurious memory access tracebacks from SPAN code even when SPAN is not configured.
  2. RP crash when unconfiguring a SPAN session with a particular session number.

Conditions: Always seen on a particular SPAN session number.

Workaround: Use a different a SPAN session number for SPAN configurations to avoid the router crash. Shutdown the SPAN session if not in use. There is no workaround to avoid spurious memory access messages.

- CSCty14596

  Symptoms:

  1. PIM neighbor is not established over routed pseudowire.
  2. PW cannot pass PIM traffic when destination LTL in DBUS header is 0x7ff8.

  Conditions: These symptoms are seen under the following conditions:

  - Configure PIM over routed pseudowire.
  - -Core facing card is ES+.
  - Outgoing interface of the PW is a TE Tunnel over the physical interface.
  - Cisco IOS 15.0(1)S and later releases.

  Workaround: Make the outgoing interface of PW:

  1. Over physical interface only (i.e. without tunnel).
  2. TEFRR over port-channel interface.
  3. Issue will not be observed on ES20.
  4. Issue will not be observed in Cisco IOS Release 15.0(1)S and later releases.

- CSCty21638

  Symptoms: The Cisco 3945 router crashes with the base configuration of SAF/EIGRP.

  Conditions: This symptom occurs when enabling the SAF Forwarder on the Cisco 3945 router box.

  Workaround: There is no workaround.

- CSCty24606

  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router's ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.

  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.

  Workaround: There is no workaround.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, ip mfib output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: Cisco 7600 running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to "multilink ppp".

Conditions: The symptom is observed when the interface is configured with a VRF.

Workaround: Shut down the interface before making the encap configuration change.

- CSCty34020

  Symptoms: A Cisco 7201 router's GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This only occurs on Gig0/3 and possibly Fa0/0 as they both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty38305

  Symptoms: The **xconnect vfi vpls** command gets rejected.

  Conditions: This symptom occurs while configuring "xconnect vfi vpls" under the interface VLAN. The error message "command rejected" is received.

  Workaround: There is no workaround.

- CSCty45999

  Symptoms: The "aps group acr 1" line disappears after power off and on a Cisco 7600 router in working and protection groups.

  Conditions: This symptom occurs when the Cisco 7600 router suddenly loses power, and the "aps group acr 1" line does not appear again. If you run the **show controller SONET 1/1/0** command, you will see every E1 on "unconfigured" status.

  Workaround: Delete the "aps protect 1 X.X.X.X" and "aps working 1" lines. The "framing" must be changed in order to delete every E1 channel configuration, then "framing" should be configured as it was in the beginning. Then "aps group acr 1" line is configured as well as "aps protect 1 X.X.X.X" and "aps working 1" lines. Finally every E1 must be configured as it was before this issue occurs. You can copy the E1 configuration before to delete anything and then paste it at the end.

- CSCty51172

  Symptoms: The MAC address learned on L2 DEC on 7600-ES+40G3CXL is not installed as the primary entry on all the member interfaces, if the ingress traffic is on the non-hashed interface for that EFP.

  Conditions: Layer 2 distributed EtherChannel traffic is learned on a hashed interface first and then moved to a non-hashed interface.

  Workaround: Do not use Layer 2 distributed EtherChannel.

- CSCty53654

  Symptoms: Traffic through 6RD tunnel is getting dropped. In the **show mls cef ipv6** *prefix* **detail** command, vlan *vlanid* field will be present. On ES+ line card, the **show platform npc 6rd egress-table vlan** *vlanid* command does not produce any output.

  Conditions: This symptom occurs when using the **clear ipv6 neighbors** command.

  Workaround: There is no workaround.

- CSCty54885

  Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.

  Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.

  Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  - The OSPF router is configured for “nsr”.
  - **Shutdown/no shutdown** of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

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

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCtz01361

  Symptoms: Traffic gets black holed when TE auto-backup is enabled on midpoint router and FFR is configured on the P2MP TE tunnel head end.

  Conditions: This symptom is seen when enabling FRR on the head end with auto- backup already configured on the box.

  Workaround: Remove auto-backup configuration from the midpoint router.

- CSCtz06611

  Symptoms: IPSec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

  Conditions: This symptom is a timing issue. You may see it first time or need to try multiple times. This symptom is seen with crypto map plus vrf configuration.

  1. Reload the router with above configuration: the mac-address changes to all FF.
  2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF.
  3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

  Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

  Workaround 1: Remove and add “ip vrf forwarding” and then remove and add the **crypto engine** command.

  Workaround 2: Remove and add the **crypto engine** command.

  Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08746

  Symptoms: On the 12in1 Serial SPA with hardware version lower than 2.0, an upgrade using “test upgrade” with the latest Cisco 7600 FPD bundles results in the SPA FPD device being downgraded from version 1.2 to 1.1. Subsequently, both auto and manual upgrades fail to bring the SPA FPD version back to 1.2. The SPA goes to the OutOfServ or FpdUpReqd state.

  Conditions: This issue is seen only with the older SPA hardware (hardware version lower than 2.0) when it is plugged into a SIP200 or SIP400 on the Cisco 7600 platform.

  Workaround: Use the latest SPA hardware (hardware version 2.0 or above).

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz24047

  Symptoms: Free process memory is being depleted slowly on line cards in the presence of the DLFIoATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the **show memory proc stat history** command to display the history of free process memory.

  Conditions: Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has DLFIoATM configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300 seconds.

  mpls traffic-eng reoptimize timers delay cleanup 300

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the “show hw-module slot X tech- support” or “show platform hardware version” command.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the “show hw-module slot X tech-support” or “show platform hardware version” command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

  Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz54823

  Symptoms: Configuration is getting locked on chopper SPA.

  Conditions: This symptom happens as follows:

  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.

  Workaround: There is no workaround. Erase start up and reload the system to get back to configuration mode.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: When service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz72615

  Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

  Conditions: This symptom is observed on Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz80643

  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz85907

  Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now if “address-family ipv6” is configured under the VRF definition, MVPN traffic might be affected.

  Conditions: SREx and RLSx releases.

  Workaround: Use ingress replication.

- CSCtz89485

  Symptoms: NAT traffic passes through the new standby router following HSRP switchover.

  Conditions: This symptom is observed with HA NAT (NAT with HSRP) mappings with inside global addresses that overlap a subnet owned by a router interface.

  Workaround:

  1. Force a HSRP switchover so that the initial standby router takes activity.
  2. Remove and re-add HSRP NAT mappings on the newly active router.
  3. Force a HSRP switchover back to the initial active router.

- CSCtz97755

  Symptoms: ES card crash and alignment tracebacks on SP are seen.

  Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running. Unconfiguring IPv6 unicast-routing will lead to this issue.

  Workaround: There is no workaround.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua13418

  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

  int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp

  int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua30259

  Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

  Conditions: This symptom occurs when SPAN is configured on service instance.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “No-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua41464

  Symptom: LC crash is seen with script run.

  Conditions: This symptom occurs when the script configures 50 MVPN GRE VRFS, 50 MLDP VRFS, with 100 mroutes each. Crash happens when traffic is sent.

  Workaround: There is no workaround.

- CSCua42089

  Symptoms: Configuring Ingress redirection for service group 61 (Mask) and applying an extended ACL in the outbound direction on the same interface causes software switching even when there are no punt entries in the TCAM.

  Conditions: This symptom is observed when WCCP service 61 with Mask assignment in the Ingress indirection, along with an outbound ACL, is configured on the same interface.

  Workaround: Do not configure the outbound ACL along with a WCCP service.

- CSCua64700

  Symptoms: IPSec tunnel states go to Up-Idle after 4-5 days of router up and running.

  Conditions: This symptom is observed if you have low re-key value. The chances of hitting this issue is high, as with the re-key the new spi gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter with the **show crypto ace spi** command.

  If no decrement in spi allocated counter and there is the consistent increment in counter, the chances are high, you will hit this issue.

  Once the value reaches to 61439, you will hit this issue.

```
MTCVPNK03#sh cry ace spi
SPI in use ........................... 0
Normal SPI allocated ................. 61439
```

  Workaround: There is no workaround.

- CSCua88341

  Symptoms: Multicast traffic on P2P GRE tunnel will get dropped.

  Conditions: This symptom usually happens in scenarios where SSO is done after vrf del/add. Here the P2P GRE tunnel will be in the VRF.

  Workaround: **shut/no shut** of the P2P GRE tunnel interface.

Resolved Caveats—Cisco IOS Release 15.1(3)S3

Cisco IOS Release 15.1(3)S3 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S3 but may be open in previous Cisco IOS releases.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCtd86428

  Symptoms: SSH session does not accept IPv6 addresses in a VRF interface, but will accept IPv4 addresses.

  Conditions: The symptom is observed when you specify the VRF name with an SSH that belongs to an IPv6 interface.

  Workaround: You can specify the source interface.

  Further Problem Description: SSH sessions not accept IPv6 addresses in VRF interface, but accepts IPv4 address:

  - Telnet session accepts both v6 and v4 addresses in VRF interface.
  - “Destination unreachable; gateway or host down” message shows in SSH session to IPv6 address in VRF interface.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

Workaround: There is no workaround.

- CSCti00319

  Symptom 1: The warning message “Fatal error FIFO” occurs repeatedly upon PPPoEoA Session teardown.

  Symptom 2: On the LC console, the message “Command Indication Q wrapped” keeps appearing.

  Conditions: This symptom is observed on a Cisco ASR1001 router and kingpin router chassis under the following conditions:

  1. High scale session counts.
  2. Range configuration with more than 100 virtual channels (VC).
  3. Back to back creation and deletion of multiple VCs with no time gap.

  Workaround: There is no workaround.

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash: on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the subinterface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtj95685

  Symptoms: A router configured as a voice gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a voice gateway.

  Workaround: There is no workaround.

- CSCtn02372

  Symptoms: QoS installation fails on the CEoP SPA or traffic is not forwarded correctly after a lot of dynamic changes that continuously remove and add VCs, as on CEoP SPA, IfIDs are not freed upon deleting the PVC.

  Conditions: This symptom occurs when continuous bring-up and tear down of VCs causes the SPA to run out of IfIDs.

  Workaround: Reload the Cisco SIP-400 line card.

- CSCtq09712

  Symptoms: A Cisco ASR’s RP crashes due to L2TP management daemon:

```
%Exception to IOS: Frame pointer 0xXXXXXXXXXXXX, PC = 0xZZZZZZZZ IOS Thread backtrace:
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = L2TP mgmt daemon
```

Conditions: This symptom is observed with L2TP when clearing the virtual access interfaces.

Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

  Conditions: The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure “ip routing protocol purge interface”.

- CSCtq77024

  Symptoms: Metrics collection fails on hop0 if route change event occurs.

  Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.

  Workaround 1: Remove and reschedule mediatrace session.

  Workaround 2: Remove and reconfigure mediatrace responder.

- CSCtq99488

  Symptoms: Session is poisoned on standby RP after performing account-logon on native IPv6 session.

  Conditions: The symptom is observed upon doing an account-logon on an unauthenticated IPv6 session with L4R applied. The session gets poisoned on the standby. The operation is, however, successful on the active RP.

  Workaround: There is no workaround.

- CSCtr06882

  Symptoms: In some cases, multicast traffic stops to flow on some subinterfaces upon router reload.

  Conditions: This symptom is observed with Cisco IOS Release RLS7.3a.

  Workaround: Perform shut/no shut of the subinterface.

- CSCtr47317

  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.

  Conditions: The issue is seen after the following sequence:

  – An internal service module session for a FWSM or other service modules exists:

```
UUT#show monitor session all
Session 1
Type : Service Module Session
```

  – If you attempt to configure a span session with the session number already in use:

```
UUT(config)#monitor session 1 source interface Gi2/7 , Gi2/40
% Session 1 used by service module
```

  - The command seems to be rejected, but it is synchronized to the standby supervisor.
  - A switchover happens.

  Workaround: There is no workaround.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

  Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr52740

  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

  Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.

  Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- CSCtr79905

  Symptoms: Error message seen while detaching and reattaching a service policy on an EVC interface.

  Conditions: The symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.

  Workaround: There is no workaround.

- CSCtr87070

  Symptoms: Enable login failed with error “% Error in authentication”.

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove “import-route target” and reconfigure route-target.

Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  ```
  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
  heartbeats
  ```

  Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

  Workaround: There is no workaround.

- CSCts15034

  Symptoms: A crash is seen at dhcpd_forward_request.

  Conditions: This symptom is observed with the DHCP relay feature when it is used with a scaled configuration and significant number of DHCP relay bindings.

  Workaround: If possible, from a functional point of view, remove the **ip dhcp relay information option vpn** command. Otherwise, there is no workaround.

- CSCts31111

  Symptoms: Coredump generation fails on the Cisco 800.

  Conditions: This symptom occurs when coredump is configured.

  Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

  ```
  conf t
  config-reg 0x0
  end
  wr
  reload
  yes
  <rommon prompt>
  DISABLE_WATCHDOG=yes
  sync
  set
  conf-reg 0x2102
  reset
  ```

- CSCts57108

  Symptoms: Standby reloads continuously after ISSU RV.

Conditions: The symptom is observed during a downgrade scenario where the active is running Cisco IOS Release 15.1 and the standby is running Release 12.2. Cisco IOS Release 15.1 will be syncing “snmp-server enable traps ipsla” keyword to the standby, but the standby does not understand the new keyword.

Workaround: Remove references to “snmp-server enable traps ipsla” and then perform the downgrade.

- CSCts59564

  Symptoms: PIM neighbor over MDT tunnel goes down.

  Conditions: The symptom is observed with **hw-module reset** of access and core card, followed by an SSO.

  Workaround: There is no workaround.

- CSCts65564

  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This only occurs if CRL caching is disabled (with the command **crl cache none** under the pki trustpoint configuration).

  Workaround: Enable CRL caching (this is the configured default).

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and re-add the **neighbor default- originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts71958

  Symptoms: When the router is reloaded due to crash, the **show version** output shows the reload reason as below:

  ```
  Last reload reason: Critical software exception, check
  bootflash:crashinfo_RP_00_00_20110913-144633-PDT
  ```

  After this, the same reason is shown even if the router is reloaded several times using the **reload** command.

  Conditions: The issue seen after a crash.

  Workaround: There is no workaround.

- CSCts97856

  Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  – On 64-bit platform systems.

  – When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt36757

  Symptoms: The following error message is noticed when configuring QoS on the interface of an ES+ card:

  ```
  %X40G_QOS-DFC9-3-CFN: qos tcam programming failed for policymap
  AGGR-CHA-INTERFACE-OUTPUT-POLICY
  ```

Conditions: The symptom is observed after a misconfiguration in the interface. The interface was misconfigured as switchport which removed the QoS configuration from the interface configuration but not from the linecard. After the interface was configured back to an L3 port, the issue started occurring when the same policy was reapplied.

Workaround: A new policy can be applied but the required policy cannot be applied again.

- CSCtt37516

  Symptoms: Linecard crash with priority traffic when QoS policy is applied.

  Conditions: The symptom is observed with the QoS priority feature.

  Workaround: There is no workaround.

- CSCtt39944

  Symptoms: The **show mls cef adjacency usage** is not showing the adjacency count correctly.

  Conditions: The symptom is observed in highly scaled networks. The platform code is not counting the last non-stats region allocation for adjacency usage.

  Workaround: There is no workaround.

- CSCtt43834

  Symptoms: Netflow counter gets incremented when sending SSM group range as v2.

  Conditions: The symptom is observed when doing an SSO.

  Workaround: There is no workaround.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt46638

  Symptoms: A Cisco 7604 running Cisco IOS Release 12.2(33)SRE4/SRE5 crashes when changing the tunnel source and destination of an IPsec sVTI.

  Conditions: The symptom is observed once the IPsec session is up and traffic is flowing through. If the tunnel source or destination is changed, the router crashes. This does not occur with a plain GRE tunnel.

  Workaround: There is no workaround.

- CSCtu00699

  Symptoms: On a DMVPN hub router, the IOS processor memory pool can get fragmented due to memory allocated for “Crypto NAS Port ID”.

  Conditions: This happens when there is network instability potentially causing tunnels to flap frequently.

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

Workaround: There is no workaround.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the linecard via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu38244

  Symptoms: After bootup, the GM cannot register and is stuck in "registering" state. Issuing the **clear crypto gdoi** command is required for a successful registration to the keyserver.

  Conditions: The symptom is observed upon router bootup.

  Workaround: Either do a **clear crypto gdoi** after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu39819

  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.

  Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

  The image used is "asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin".

  Workaround: There is no workaround.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu51904

  Symptoms: You can observe decrementing free memory by each repetition of the process by using the **show memory statistics** command under the active SP.

  Conditions: The symptom is observed by removing "default mdt" under the VRF configuration and then adding it back. The memory leak is recognized on the active SP.

  Workaround: Reload the router.

- CSCtu60863

  Symptoms: IGMP reports do not get installed in the IGMP group list.

  Conditions: The symptom is observed when the port-security feature is enabled on the switchport which is part of the VLAN on which the IGMP reports are received.

Workaround: Remove “switchport port-security” from ports associated with the VLAN on which the IGMP reports are received.

- CSCtw45055

  Symptoms: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold
time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session  Neighbor deleted
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
```

  The scheduler process will attempt to reference a freed data structure, causing the system to crash.

  Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

  Workaround: There is no workaround.

- CSCtw46625

  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).

  Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

  Workaround: Force the QL PRC value by executing the following command:

  network-clock quality-level rx QL-PRC controller SONET 1/2/0

- CSCtw48209

  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

  Workaround: There is no workaround.

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw64040

  Symptoms: Crash due to MPLS, which appears to be associated with load- balancing.

  Conditions: This symptom occurs when MPLS is configured.

  Workaround: There is no workaround.

- CSCtw71564

  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.

  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.

  Workaround: Reduce processor load on device running the responder.

- CSCtw72708

  Symptoms: Malloc failure, CPU hog, and memory leaks are seen creating the MD entry with your own IP address as the next-hop listener.

  Conditions: Issue is seen on a Cisco 7600 series router that is running Cisco IOS 15.2(04)S version. There are two triggers:

  1. When LI is configured on the Cisco 7600 with the remote’s MDip as one of your own; resulting in CPU hog and memory failures.
  2. When one generic stream is deleted, an internal counter is decremented twice. Thus disabling the LI feature even when there is another active tap installed.

  Workaround: Configure the MD listener IP address with the correct IP address.

- CSCtw76044

  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.

  Conditions: The symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw88094

  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.

  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.

  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- CSCtw94598

  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.

  Conditions: The symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.

  Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```

  but instead it shows:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1
  ```

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtw99989

  Symptoms: During normal operation a Cisco ASR 1000 Series Aggregation Services router may show the following traceback:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi
  ```

  Conditions: The symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx18626

  Symptoms: IPv6 BFD hardware offloaded sessions do not come up when BFD session is formed.

  Conditions: The symptom is observed when an IPv6 BFD session is created between a Cisco 7600 (in one side) and third party vendor devices (on the other side).

  Workaround: There is no workaround.

- CSCtx21206

  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1..

  Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- CSCtx28483

  Symptoms: A router set up for Cisco Unified Border Element-Enterprise (CUBE- Ent) box-to-box redundancy will reload when certain configuration commands are deconfigured out of the recommended sequence.

  Conditions: The symptom is observed when deconfiguring CUBE-Ent box-to-box redundancy once it is already configured (for CUBE-Ent box-to-box redundancy) on the Cisco ASR platform. You cannot change the configuration under the “application redundancy group” submode without first

removing the redundancy-group association under “voice service voip” submode. If you do not remove this association first before changing the configuration under “application redundancy group”, the ASR will reload. You are not provided any other option.

Workaround: Always first remove the redundancy-group association under “voice service voip” submode first and then you can change the configuration under “application redundancy group”.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exists.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when doing **show ip route** command or when default route is updated.

  Workaround: There are two possible workarounds:

  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCtx29557

  Symptoms: A standby crashes @ fib_fib_src_interface_sb_init.

  Conditions: All.

  Workaround: There is no workaround.

- CSCtx31175

  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.

  Conditions: The symptom is observed with the following conditions:

  1. User session exists on ASR1001.
  2. Stop one user’s session by using **clear subscriber session username xxx** on ASR1001.
  3. ASR1001 sends double “Framed-IP-Address” in service-stop accounting for one user’s session.

  Workaround: Do not use **clear subscriber session** command to clear the session, instead use **clear pppoe**.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - **address family vpnv4** is enabled.
  - **address family ipv4 mdt** is enabled.

  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx35692

  Symptoms: On the Cisco ASR 1000 platform, while acting in a redundancy pair, when the standby ASR becomes active the dial-peers on the standby never change their state back to active causing all calls to fail. Calls that were active during the failover scenario will stay active in the new switchover. Only new calls are affected.

  Conditions: The symptom is observed on an ASR 1000 series router CUBE with a box-to-box redundancy configured that is using OOD option pings in the dial- peers. Global configuration of option pings under voice service VoIP is only for IN-Dialog option pings.

  Workaround: Disable option keepalives from the dial-peers.

- CSCtx39936

  Symptoms: A Cisco 7600 router configured for MPLS TE with tunnel load-sharing may punt traffic to MSFC when multiple TE paths to a given destination exist.

  Conditions: The symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE4, configured with multiple MPLS TE tunnels with load-sharing.

  Workaround 1: In some cases, clearing the router may trigger proper reprogramming of the prefix in the hardware.

  Workaround 2: Remove load-sharing from the TE tunnels.

- CSCtx47213

  Symptoms: The following symptoms are observed:

  1. Session flap when iBGP local-as is being used on RRs.
  2. Replace-as knob is not working in iBGP local-as case.

  Conditions:

  1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
  2. Replace-as knob even used is ignored and prefixes are appended with local-as.

  Workaround: Do not use iBGP local-as.

- CSCtx48010

  Symptoms: PIM neighbors on MDT tunnel continuously flap on a Cisco 7600 series router. Decapsulation path shows wrong rewrite index for flapping peers, instead of expected 7FFA recirculation index.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)S1. ES20 card as core-facing.

  Workaround: Identifying the adjacency of the flapping peer and changing the rewrite index to 7FFA manually stops the flap:

  ```
  test mls cef adj 180262 4055 9238 7ffa 2608 20 multicast 001e.f741.e28d 0.0.0 0 0x5fa
  ```

- CSCtx51935

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: The symptom is observed with the following steps:

  ```
  interface gi1/2
  mpls traffic-eng tunnels
  no shut
  ```

```
router OSPF 1
mpls traffic-eng area 100
mpls traffic-eng router-id lo0
end
```

Workaround: There is no workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through “ip multicast boundary”.

  Conditions: The symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use “no ip pim autorp” which will disable Auto RP completely from this device.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx71618

  Symptoms: Router crash at process L2TP mgmt daemon.

  Conditions: The symptom is observed with a Cisco ASR 1006 (RP2) running Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCtx73452

  Symptoms: The following symptoms are observed:

  1. You send an ICMPv4 packet with IP option. It will be forwarded by ASR1001. IP options field includes “loose source routing” option.
  2. ASR 1001 receives the packet. ASR 1001 has “no ip source-route” setting in its configuration.
  3. ASR 1001 incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.

  Conditions: The symptom is observed with the Cisco ASR 1001 (2.5G ESP).

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx89018

  Symptoms: MLDP MVPN traffic over data MDTS is dropped.

  Conditions: The symptom is observed with the following conditions:

  - Multicast traffic is flowing on data MDTS.
  - The issue is seen after second switchover but sometimes on first switchover.
  - Multicast scale is 40 VRFs with 10000 mroutes distributed unequally among the 40 VRFs.

  Workaround: Using **clear ip mroute *** in all the VRFs will recreate all the mroutes and traffic will be resumed.

- CSCtx99544

  Symptoms: Exception occurs when using **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3*:

  ```
  router(config)# no ip vrf VRF3
  router(config)# no aaa accounting system default vrf VRF3 start-stop group
  RADIUS-SG-VRF3

  %Software-forced reload
  ```

  Conditions: The symptom is observed with the following conditions:

  - Hardware: Cisco ASR 1001.
  - Software: asr1001-universalk9.03.04.02.S.151-3.S2.

  Workaround: There is no workaround.

- CSCty02403

  Symptoms: EIGRP topo entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also be flapped.

  Conditions: It can only occur when you have more then one attribute set in any route received from a neighbor.

  Workaround: Do not set more then one attribute in the route.

- CSCty16623

  Symptoms: Traffic getting black holed because the VPN corresponding to the tunnel secondary VLAN gets programmed with punt adjacency.

  Conditions: The symptom is observed with unconfiguring-reconfiguring the VRF. (The issue is independent of time gap between the configuration change.)

  Workaround: There is no workaround.

- CSCty34109

  Symptoms: Router crash at pm_port_set_vlan_state.

  Conditions: The symptom is observed with the following conditions:

  - 50 GRE-based MVPN intranet MVRFs with 100 mroutes in each, with PIM-SM having static-RP in core for 25 MDTs and auto-RP for 25 MDTs and PIM-SSM in VRF.
  - 50 MLDP-based intranet MVRFs with 100 mroutes in each, with PIM-SM having static-RP in 25 VRFs and auto-RP in 25 VRFs.
  - 100 P2MP-TE tunnels, with explicit paths. One branching point at nPE1, nPE2, nPE3, nPE4, uPE1, uPE2 and six branching points at nP with nP as bud node.
  - 900 unicast VRFs.

  - 5K mroutes in global context (plain multicast with PIM-SM having static RP for RP election).
  - IGP as OSPF.
  - P2P-TE tunnels in core, with link FRR protection.

  Workaround: There is no workaround.

- CSCty37445

  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: The symptom is observed when on the spoke you have a **distribute list route-map** command setting tags.

  Workaround: Once you remove that command EIGRP works normally.

- CSCty41067

  Symptoms: Router crashes while doing an SSO without any configurations.

  Conditions: The symptom is observed while doing an SSO.

  Workaround: There is no workaround.

- CSCty58656

  Symptoms: A Cisco 7600 series router with ES+ module may crash.

  Conditions: The symptom is observed with the QoS policy map that has a name hash that is same as an existing policy used by the ES+ module and configuring a child policy or adding a child policy that is already in use.

  Workaround: Do not call a child policy map.

Resolved Caveats—Cisco IOS Release 15.1(3)S2

Cisco IOS Release 15.1(3)S2 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S2 but may be open in previous Cisco IOS releases.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCsh39289

  Symptoms: A router may crash under a certain specific set of events.

  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCta27728

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed on a Cisco ASR1002 router running Cisco IOS Release 15.1(2)S1 with RSVP for MPLS TE tunnel signaling.

  Workaround: There is no workaround.

- CSCtc96631

  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.

  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.

  Workaround: Use Cisco ASRs instead of Cisco ISRs.

- CSCti33159

  Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.

  Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.

  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.

- CSCtj33003

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

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

  This advisory is available at the following link:

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

- CSCtk03371

  Symptoms: SVI-based EoMPLS/VPLS VC fails to forward traffic even when VC is up.

Conditions: This happens when the **ip cef accounting non-recursive** command is configured on the router. This command is documented as an unsupported command on the Cisco 7600 platform, but it should also generate an error message when configured on the Cisco 7600. Preferably it should not take any action, for example, it should not affect any other working features.

Workaround: Unconfigure the command by typing “no ip cef accounting non- recursive”.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

  Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

  Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl83517

  Symptoms: The last switchover redundancy mode shows the configured mode.

  Conditions: This symptom occurs if DIVC ISSU results puts the system in RPR mode, and the last switchover redundancy mode still shows SSO. When a system tries to come out of RPR to SSO through either manual reset of standby or OIR, it will be stuck in RPR and will not progress to SSO as the last switchover flag shows SSO, and clients assume it is already in SSO.

  Workaround: There is no workaround.

- CSCtn04357

  Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

  vlan configuration 161 ip flow monitor flowmonitor1 in ip flow monitor flowmonitor1 input

  Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

  Workaround 1: Remove the flow monitor configuration.

Workaround 2: Use netflow-v9 export protocol.

Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn07696

  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

  Conditions: This symptom is observed with the following CLI:

  ```
  show tech-support | redirect
  ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```

  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn31333

  Symptoms: High CPU utilization is observed on the Cisco CMTS router due to the Net Background process.

  Conditions: This symptom is observed on a router used for L2TP network server (LNS) with an L2TP application.

  Workaround: There is no workaround.

- CSCtn59075

  Symptoms: A router may crash.

  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.

  Workaround: Disable Flexible NetFlow on all interfaces.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCto81701

  Symptoms: The PfR MC and BR sessions flap.

  Conditions: The symptom is observed with a scale of more than 800 learned TCs.

  Workaround: Use the following configuration:

  pfr master keepalive 1000

- CSCto88393

  Symptoms: CPU hogs are observed on a master controller:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0),process
  = OER Master Controller.
  ```

  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

  Workaround: There is no workaround.

- CSCtq29547

  Symptoms: The router crashes on watchdog timeout while processing the SNMP request for ciscoEigrpMIB.

  Conditions: This symptom occurs while processing the SNMP request for ciscoEigrpMIB.

  Workaround: Exclude ciscoEigrpMIB from being polled by using the following SNMP view:

  ```
  snmp-server view NOCRASH internet included
  snmp-server view NOCRASH ciscoEigrpMIB excluded
  ```

  Then, apply the view to your SNMP community string: snmp-server community test view NOCRASH

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq60703

  Symptoms: The device crashes and traceback is seen when executing **write network**.

  Conditions: The symptom is observed when the command **write network** is used with no URL specified.

  Workaround: Specify a URL.

- CSCtq61128

  Symptom: Router is crashing with Segmentation fault (11).

  Conditions: This symptom is observed on routers acting as IPSEC hub using certificates.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:

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

CVE ID CVE-2011-4231 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

- CSCtq68778

  Symptoms: After an ISSU, the reload reason string is missing in the newly-active session.

  Conditions: The symptom is observed after an ISSU.

  Workaround: There is no workaround.

- CSCtq88777

  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

  Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

  Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtr04829

  Symptoms: A device configured with "ip helper-address" drops packets because of a zero hardware address check.

  Conditions: This symptom occurs when the hardware address is zero.

  Workaround: There is no workaround.

- CSCtr05686

  Symptoms: An error occurs when a policy-map with byte based queue-limit is not attachable to target.

```
policy-map p1
 class class-default
  bandwidth 200
  random-detect dscp-based
  random-detect dscp 8 10000 bytes 20000 bytes 10
  random-detect dscp 16 13500 bytes 20000 bytes 10
  random-detect dscp 24 16000 bytes 20000 bytes 10
  random-detect dscp 32 18000 bytes 20000 bytes 10
```

  The above configuration is not possible.

  Conditions: This issue occurs only when bytes based WRED is configured before byte based queue-limit.

Workaround: See the following:

```
policy-map p1
 class class-default
  bandwidth 200
  queue-limit 3000 bytes
  random-detect dscp-based
  random-detect dscp 8 10000 bytes 20000 bytes 10
  random-detect dscp 16 13500 bytes 20000 bytes 10
  random-detect dscp 24 16000 bytes 20000 bytes 10
  random-detect dscp 32 18000 bytes 20000 bytes 10
```

- CSCtr06926

  Symptoms: A CA server in auto grant mode goes into disabled state when it receives a client certificate enrolment request.

  Conditions: The symptom is observed when a client certificate enrolment request is received.

  Workaround: Do not place the CA server in auto grant mode.

- CSCtr25386

  Symptoms: BFDv6 static route association fails after reenabling interfaces.

  Conditions: This symptom is observed after interfaces are reenabled.

  Workaround: There is no workaround.

- CSCtr31496

  Symptoms: The line card crashes after switchover with the multilink configurations.

  Conditions: This symptom occurs after switchover with the multilink configurations.

  Workaround: There is no workaround.

- CSCtr33918

  Symptoms: Convergence is observed in the order of 1-6 seconds of multicast/video traffic on a Cisco 7600 router that is running Cisco IOS Release 15.0(1)S3a.

  Conditions: This symptom is observed with failure or restoration of a link carrying multicast/video traffic at the head-end or receiver-end.

  Workaround: There is no workaround.

- CSCtr34960

  Symptoms: A router that is running Cisco IOS may run out of IO memory.

  The **show buffers** command shows that the count reaches 0 in free list.

```
Router#sh buffers
...
Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
```

```
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

Conditions: This issue is seen post bootup. The Cisco 7600 in HA is required to hit the issue. The **show buffers old** command shows some buffers hanging on EOBC buffers list for a long time, weeks or more. The issue is a corner case, and buffer leak rate is slow.

This DDTS fixes leaks for the **mls cef maximum-routes** and **mls cef adjacency-mcast** commands.

See the output from the **show buffers old pack**:

```
F340.08.04-6500-2-dfc1#show buf old packet

Buffer information for EOBC0/0 buffer at 0x275A0B00
  data_area 0x275A0FB8, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:36.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A100C, datagramsize 50, maximum size 1680
  mac_start 0x275A0FFE, addr_start 0x275A0FFE, info_start 0x0
  network_start 0x275A100C, transport_start 0x0, caller_pc 0x205DF718

275A100C: 00200000 02010000 00010006 01000000  . ..............
275A101C: 00350001 00101608 00000053 000000A6  .5.........S...&
275A102C: 000603E7 01170000 00000000 00000000  ...g............
          --------
275A103C: 000000                               ...

Buffer information for EOBC0/0 buffer at 0x275A5B48
  data_area 0x275A6000, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:41.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A6054, datagramsize 80, maximum size 1680
  mac_start 0x275A6046, addr_start 0x275A6046, info_start 0x0
  network_start 0x275A6054, transport_start 0x0, caller_pc 0x205DF718



275A6054:          00200000 02010000 02150007      . ..........
275A6060: 01000000 000A0001 00301608 00000052  .........0.....R
275A6070: 000000A4 00480002 01047FFF 00000001  ...$.H..........
                   --------
275A6080: 00000000 00000000 00000000 00000000  ................
275A6090: 00000001 00000000 00000000 00000000  ................
275A60A0: 00000000 00
```

```
F340.08.04-6500-2-dfc1#
```

The **show buffers old packet** command output will be either 000603E7 OR 00480002.

Workaround: Reload the supervisor to clear the leaked buffers.

- CSCtr35740

  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.

  Workaround: There is no workaround.

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

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

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

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

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

  Workaround 1: Enable IPv6 explicitly on the main interface:

  ```
  interface x/y
    ipv6 enable
  ```

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

  ```
  interface x/y.z
    no ipv6 address
    ipv6 address ...
  ```

- CSCtr56174

  Symptoms: The MPLS-TE link count reaches a large value (4 billion+) on the Cisco ASR 1000 series router and negative value on the Cisco 7600 series router. This issue is seen in the **show mpls tr link sum** and **show mpls tr link int** command output.

  Conditions: This symptom occurs if MPLS-TE tunnels are deleted using the **no int tunX** command and if the number of TE tunnels deleted are more than the TE links on the box. Even if they are not, with every TE tunnel deleted, the link count is affected and gets reduced.

  Workaround: Do not delete MPLS-TE tunnels using the **no int tuX** command. If a TE tunnel is not required, shut it down. If these symptoms are observed, the only way is to reboot.

- CSCtr58140

  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

Workaround: There is no workaround.

- CSCtr79347

  Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
  Traceback summary
  % 0x80e7b6 : __be_bgp_tx_walker_process
  % 0x80e3bc : __be_bgp_tx_generate_updates_task
  % 0x7f8891 : __be_bgp_task_scheduler
  ```

  Conditions: No conditions but this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr81559

  Symptoms: The PPP session fails to come up occasionally on LNS due to a matching magic number.

  Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.

  Workaround: To avoid this, renegotiate the LCP. Configure the client using the **retry** command. This may cause the next session to come up correctly.

- CSCtr91106

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

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

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

- CSCtr91890

  Symptoms: An RP crashes sometimes when the router is having PPPoX sessions.

  Conditions: If a PPPoX session is terminated in the middle of session establishment and ip local pool is configured to pick the IP address for the peer and the version that the router is running has the fix for CSCtr91890.

  Workaround: There is no known workaround.

- CSCtr92285

  Symptoms: The following log is seen, and VCs cannot be configured.

  ```
  SSM CM: SSM switch id 0 [0x0] allocated
  ACLIB [Gi9/1/0.3830, 3830]: Failed to setup switching for VLAN interface ...
  ```

Conditions: This symptom is observed with the access circuit interface shut and core flaps occurring, along with pseudowire redundancy. Also, leaks occur per flap.

Workaround: There is no workaround. If VCs can be removed, do so to release some IDs. Otherwise, try a redundancy switchover.

- CSCtr94545

  Symptoms: Standby crashes at fm_global_feature_add_for_vrf.

  Conditions: The system crashes when virtual servers are deleted.

  Workaround: There is no workaround.

- CSCts06929

  Symptoms: Disposition traffic gets dropped after SSO as the new local labels allocated by AToM do not get programmed on the line cards.

  Conditions: This symptom occurs when pseudowires are configured on the setup without graceful restart configured. Then, SSO is performed and two local labels have the same disposition information. This really manifests as a traffic drop issue when the scale is high.

  Workaround: Configuring graceful restart resolves this issue.

- CSCts11594

  Symptoms: A mediatrace session is scheduled with an attached session- parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.

  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.

  Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.

  Workaround: Use either the default session-parameters or custom session- parameters. Do not toggle between both.

- CSCts16013

  Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1K router. RP crash occurs due to memory leak by the QOS Accounting feature.

  Conditions: This symptom is observed during testing with the QOS Accounting feature PAC2. This issue is seen when there are a large number of sessions and churns with “aaa-accounting” in the QOS policy-map.

  Workaround: There is no workaround.

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts20246

  Symptoms: The DR for the receiver segment forwards IPv6 multicast packets on the Accepting Interface of S,G.

Conditions: This symptom occurs while multicast stream is running and the RPF interface towards the source and RP goes down on the DR and the interface connected to the receiver (oif in S,G before interface goes down) becomes the RPF interface for the source and RP and hence iif for S,G.

Workaround: There is no workaround.

- CSCts27042

  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

  Workaround: There is no workaround.

- CSCts32920

  Symptoms: Traffic gets punted to the RP.

  Conditions: This symptom occurs when there are multiple P2P-GRE tunnels in a particular VRF. Remove one particular P2P-GRE tunnel from that VRF.

  Workaround: Shut/no shut P2P-GRE tunnels in that particular VRF, for which traffic is getting punted to the RP.

- CSCts34693

  Symptoms: A Cisco router may crash with the following error message:

```
000199: *Aug 23 16:49:32 GMT: %BGP-5-ADJCHANGE: neighbor x.x.x.x  Up

Exception to IOS Thread:
Frame pointer 0x30CF1428, PC = 0x148FDF84

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog
-Traceback=
1#07279b80de945124c720ef5414c32a90  :10000000+48FDF84 :10000000+48FE400 :10000
000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FE
F0 :10000000+F5FF94 :10000000+F60608
```

  Conditions: This symptom is observed in a Cisco ASR 1004 router that is running Cisco IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.

```
event manager applet BGP-MON
 event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down"
 event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up"
trigger
  correlate event BGP-DOWN or event BGP-UP
 action 02 cli command "enable"
 action 03 cli command "sh log"
 action 04 mail server "$_email_server" to "$_email_to" from
"$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername,
BGP neighbor Change" body "$_cli_result"
```

  Workaround: There is no workaround at this time.

- CSCts38429

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

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

- CSCts41217

  Symptoms: Memory leak occurs in const_mfib_lc_* processes.

  Conditions: This symptom is observed during deletion and addition of VRFs. Multicast needs to be enabled in the VRF and the P2P tunnels should be present in the VRF. VRF should be removed before deleting the P2P tunnels for this to happen.

  Workaround: Delete all the P2P tunnels before removing the VRF

- CSCts42154

  Symptoms: After the Cisco IOS ASR 1006 router is reloaded, it fails to reregister to the key server. From the debugs, it is observed that the attempt to register is generated too early before the GDOI is ON. This registration attempt is made before the interface, through which GDOI registration traffic with the key server passes, goes to the UP state.

  Conditions: This symptom is observed on a Cisco IOS ASR 1006 router that runs Cisco IOS Release 15.0(1)S2 and Cisco IOS Release 15.0(1)S3.

  Workaround: Use the **clear crypto gdoi** command to fix this issue.

- CSCts47566

  Symptoms: During standby RP bootup, an incorrect ICMP punt entry for MPLS interfaces gets programmed. This entry appears even if the interface has no ACL applied in the input/output direction.

```
2037#show tcam inter gi4/0/3 acl in ip

* Global Defaults shared


Entries from Bank 0

    punt          icmp any any eq 11 <<<<<<<<<<<<<<<<
    permit        ip any any (1895 matches)

Entries from Bank 1
```

  Conditions: This symptom is observed with the ICMP punt entry, which is required to allow trace route across MPLS cloud. This is a workaround for a hardware problem with Tycho. The feature is called “FM_FEATURE_MPLS_ICMP_BRIDGE”. This workaround is required only if there are aggregate labels programmed in the superman VPN cam, but can get set incorrectly even when there is no VRF configuration on the box.

  Workaround: To clear the entry set unnecessarily, disable/enable MPLS on the interface for which it appears.

- CSCts49032

  Symptoms: Data traffic is getting block-holed.

Conditions: This symptom occurs with the removal/addition of default MDT address in VRF, with time gap of 30 minutes.

Workaround: Deletion/addition of VRF.

- CSCts55322

  Symptoms: More traffic is sent out because of stale MET entries.

  Conditions: This symptom occurs in a scale condition when the route towards the core on the source PE is changed.

  Workaround: There is no workaround.

- CSCts57115

  Symptoms: After the following procedure is executed, multicast traffic on several VRFs is not forwarded to the outbound tunnel interface for MDT.

  The procedure is as follows:

  1. Reload the router.
  2. Perform RP switchover.
  3. Perform active ESP(F0) hardware reload.
  4. Perform active ESP(F1) hardware reload.

  Conditions: This symptom is observed when MVPN sends out multicast traffic on a lot of VRFs.

  Workaround: Use the **ip pim sparse-mode** command to reconfigure the loopback0(global) interface.

- CSCts58394

  Symptoms: The SNMP graph traffic rate (collected from the port-channel subinterface) does not match the 5-minute offered rate from “show policy-map inter port-channel x.x”.

  Conditions: This symptom occurs on the Cisco 7600-S running Cisco IOS Release 15.0(1)S4 with the port-channel subinterface on 76-ES+XC-40G3CXL. This issue is seen only when there is EARL recirculation of packets and affects only the ingress traffic rate.

  Workaround: There is no workaround.

- CSCts62082

  Symptoms: Router generates the following message:

  ```
  %NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP
  group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure
  ```

  Conditions: The symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts64539

  Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

  Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x diable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts69204

  Symptoms: PPPoE sessions do not get recreated on the standby RP.

  Conditions: This symptom occurs on the standby RP.

  Workaround: There is no workaround.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

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

- CSCts81427

  Symptoms: With a scaled dLFIoATM configuration on FlexWAN, after issuing SSO, some of the interfaces stop pinging.

  Conditions: This symptom is observed after doing SSO.

  Workaround: Shut/no shut of the ATM interface helps to resolve the problem.

- CSCts85694

  Symptoms: The following error message is displayed:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi  (0x104C2E4)
  ```

  Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak is increasing incrementally. Leak is very slow.

  Workaround 1: Do not bring down all sessions together.

  Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

  Workaround 3: Do not have accounting accuracy configured.

  Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts86788

  Symptoms: CPU Hog messages start to appear followed by a crash.

  Conditions: This symptom is observed when the **show mpls traffic-eng fast-reroute database interface** *name* **detail** command is issued on an interface where there are no MPLS-TE tunnels.

  Workaround: Do not issue this command on an interface where there are no MPLS-TE tunnels.

  Further Problem Description: The trigger is simple, that is, issuing the FRR **show display** command on an interface on which there are no MPLS-TE tunnels.

- CSCts88467

  Symptoms: The drops happen earlier than expected.

  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.

  Workaround: Configure a queue-limit explicitly to fix this issue.

- CSCts90734

  Symptoms: IKEA message trace entry memory leak is seen.

  Conditions: This symptom occurs when there is an IPsec session.

  Workaround: There is no workaround.

- CSCts97803

  Symptoms: When a policy-map is configured with two RTP class-maps and two RTP encapsulated MDI class-maps, flows are monitored on them. Changing one of the RTP class-maps to MDI will lead to the crash. Also when a policy-map is configured with both RTP and MDI class-maps, and if the flow being monitored by them is RTP encapsulated MDI flows, then RTP monitoring will not work.

  Conditions: This symptom is seen when policy-map is configured with both RTP and MDI class-maps. The RTP flow to be monitored should be RTP encapsulated MDI flow.

  Workaround: There is no workaround.

- CSCtt03485

  Symptoms: ES40: IDBMAN crash is seen with “no ip flow-export destination <> vrf <>”.

  Conditions: This symptom occurs when “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120” is removed.

```
PE2(config)#no ip flow-export destination 10.21.1.1 3000 vrf vrf_1120

PE2#show vlan internal usage | i NDE      both NDE internal VLANs 1013, 1015
are cleared  from 'internal VLAN table'

PE2#show monitor event-trace idbman all | i NDE
*Sep 28 00:21:58.523: clear NDE_1013 vlan 1013
*Sep 28 00:21:58.527: clear NDE_1013 vlan 1013  mapping 1013 is cleared, but
 1015  is not cleared from idbman mapping

PE2#test platform debugger callfn name idbman_dump_vlans 0
Calling address (0x0AF46AFC) 1: Vl1 : 1
1015: NDE_1015 : 1015    mapping 1015 is still present in IDBMAN, eventhough
1015 is a free VLAN, so, it can be allocated to any new interface
```

Now, 1015 can be allocated for any other new interface, as it is cleared from “internal VLAN table”, whereas it is not cleared from IDBMAN mapping. Thus, you can reproduce the IDBMAN inconsistency with NDE interfaces.

When a new interface comes UP, the IDBMAN set will fail, as there is already an old mapping existing (NDE_1015). When you try to delete this new interface, it will try to clear the mapping in IDBMAN. But, it finds the old mapping (NDE_1015); hence, you must perform forced crash in idbman_if_clear_vlan_id and configure “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120”.

```
PE2#show vlan internal usage | i NDE
1013 NDE
1015 NDE_vrf_0

PE2#show monitor event-trace idbman all | i NDE
*Sep 28 00:08:39.387: set NDE_1013 vlan 1013
*Sep 28 00:08:39.395: set NDE_1015 vlan 1015

                              PE2#test platform debugger callfn name
idbman_dump_vlans 0
                             Calling address (0x0AF46AFC) 1: Vl1 : 1
                              1013: NDE_1013 : 1013
                              1015: NDE_1015 : 1015
```

Workaround: Reload.

- CSCtt11210

  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.

  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt16487

  Symptoms: High CPU is seen when changes are made to the Cisco WCCP Access Control List (ACL).

  Conditions: This symptom is observed in a Cisco WCCP ACL.

  Workaround: There is no workaround.

- CSCtt18020

  Symptoms: A router that is running Cisco IOS may reload unexpectedly.

  Conditions: This symptom may be seen with active SSH sessions to or from the router. Only SSH is affected.

  Workaround: Use Telnet.

- CSCtt19442

  Symptoms: Cisco 7600 subinterface that is configured for bridging after router reload sends traffic even when being shutdown. This traffic is sent from physical interface to which subinterface correspond and further received on the other side of the link.

Conditions: This symptom is seen when bridging is configured on subinterface.

Workaround:

- Doing a **no shutdown**, then **shutdown** on the subinterface clears the issue.
- Remove bridging configuration from subinterface.

Deleting subinterface, and then recreating it does not fix the issue.

- CSCtt23367

  Symptoms: The status on active PoA is A/U. The status on standby PoA is S/A.

  Conditions: This symptom is seen after HA switchover. When configuring a new mLACP port-channel on new ACTIVE RP, it may get stuck in A/U state.

  Workaround: Remove the port-channel and RG configuration and add back again.

- CSCtt26532

  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

  Workaround: There is no workaround.

  Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

  Conditions: This symptom is observed on a Cisco ASR 1006 router running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image. The **show version** command causes the “Last reload reason: Critical software exception” error.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored.

  Conditions: This symptom is seen with the use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3:

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

  No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

- CSCtt32165

  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.

Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

```
show voip fpi stats | include provisn rsp


provisn rsp          0      32790        15
```

Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt33158

  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.

  Conditions: The symptom is observed if WRED is already present and the queue limit is configured in packets.

  Workaround: Remove WRED and reattach it.

- CSCtt35936

  Symptoms: EIGRP route updates are not sent to DMVPN spokes. The **show ip eigrp inter** command output shows pending routes in interface Q, which remains constant. The **show ip eigrp int deta** command output shows that the next sequence number of the interface remains the same (does not advance).

  Conditions: This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.

  Workaround: Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- CSCtt46873

  Symptoms: In an MVPN setup, when the **mdt default** command is removed from under the VRF, unicast packets coming from the core, such as LDP and BGP, get dropped, leading to router isolation.

  Conditions: This issue is primarily seen when mls mpls tunnel-recir is not configured on the box (or does not get enabled due to the absence of a sip10g device). In such a case, MDT tunnel VLAN gets allocated, but is never released, until the **mdt default** command is removed. Since the decap adjacency handling the unicast packets is a GRE decap, with an MDT tunnel VLAN allocated, removal/re-add of **mdt default** command will program the adjacency with the MDT tunnel VLAN. Another removal along with a race condition might leave the adjacency with the tunnel VLAN (now deallocated), thereby causing the unicast packets to be dropped.

  Workaround: Configure mls mpls tunnel-recir on the box and remove/re-add the **mdt default** command or reload with mls mpls tunnel-recir configured to be safe.

- CSCtt69984

  Symptoms: The Cisco ASR 1000 series router does not initialize GDOI registration for the second GDOI group after reload.

Conditions: This symptom is observed with the following conditions:

1. Image version: Cisco IOS Release 15.1(3)S
2. Platform: Cisco ASR 1000 series router
3. Two GDOI groups need to be configured.

Workaround 1: Issue the **clear crypto gdoi** after the router reloads, or remove the crypto map from the WAN interface and reapply it.

Workaround 2: If you are using the same local address for different GDOI groups, have the two groups use a different local address.

- CSCtt90672

  Symptoms: CFM MEP enters the INACTIVE state on deleting the subinterface.

  Conditions: This symptom is observed under the following conditions:

  1. Create a subinterface (vlan 104) for EOAM communication. Check “CC-Status” = Enabled.
  2. Create a QinQ subinterface (vlan tags: 104 128) for subscriber on the same physical interface. Check “CC-Status” = Enabled.
  3. Later, delete the QinQ subinterface from the step 2 above (DT’s provisioning system does it, for example, for a new policy change). The “CC-Status” goes to inactive.

  Workaround: Unconfigure and reconfigure the **continuity check** command under the corresponding Ethernet CFM domain/service global configuration for this CFM MEP.

- CSCtu01172

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document “Cisco Unified Border Element High Availability(HA) on ASR platform Configuration Example.”

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration, that is, “no application redundancy”.

- CSCtu08608

  Symptoms: The standby RP crashes due to VoIP HA Session App.

  Conditions: The Cisco ASR 1000 platform with redundant RPs and Cisco Unified Border Element Enterprise. The signature in the crashinfo is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Voip HA Session App
  ```

  Workaround: There is no workaround.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

  ```
  Router#sh buffers
  Buffer elements:
       779 in free list (500 max allowed)
       1582067902 hits, 0 misses, 619 created

  Interface buffer pools:
  ....
  ```

```
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . .............. --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............  --> ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu30649

  Symptoms: Standby is reset.

  Conditions: This issue is seen when the ISSU standby is reset because of MCL failure.

  Workaround: There is no workaround.

- CSCtu31340

  Symptoms: The **show sip call called-number** crashes the router.

  Conditions: This symptom is observed when the call SIP state is DISCONNECT.

  Workaround: There is no workaround.

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

  Conditions: This symptom is observed under the following conditions:

  – The PPPoE dialer client needs to be configured on the physical SHDSL interface.
  – The GRE tunnel destination interface should point to the dialer interface.
  – The MPLS pseudowire should go over the tunnel interface.
  – After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

  Workaround: There is no workaround.

- CSCtu36562

  Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW- MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).

  Conditions: The symptom is observed with failed IKE negotiations (ph1 or ph2).

  Workaround: There is no workaround.

- CSCtu92289

  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

  Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

  Workaround: There is no workaround.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces.
  3. if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.

  Conditions: This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa.

  Workaround: This issue is seen starting from Cisco IOS XE Release 3.2. Cisco IOS XE Release 3.1 should work fine.

- CSCtw73551

  Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

  ```
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps
  ```

  Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)S1

Cisco IOS Release 15.1(3)S1 is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S1 but may be open in previous Cisco IOS releases.

- CSCso88042

  Symptoms: The VLANs allowed on the trunk to WiSM are lost on every reload.

  Conditions: This symptom occurs when the number of entries in the allowed-VLAN statement exceeds five.

  Workaround: Limit the number of entries to five or less, using ranges instead of single VLANs.

  Further Problem Description: When the entries in the VLAN-allowed statement are more than five, two WiSM module allowed-VLAN statements are seen, even though one line was allowed during configuration. When reloaded, only one WiSM module allowed-statement is taken and the first statement is lost.

- CSCsq45560

  Symptoms: The port-channel member link stays as a standalone port with LACP.

  Conditions: This symptom is observed only with the “vlan dot1q tag native” feature enabled.

  Workaround: There is no workaround.

- CSCtd15853

  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

  Conditions:

  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

  Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

  Workaround: There is no workaround.

- CSCti83542

  Symptoms: MPLS LDP flapping is seen with T3 SATOP CEM interface configurations.

  Conditions: This issue is seen with T3/E3 SATOP TDM configurations.

  Workaround: There is no workaround.

- CSCtj56551

  Symptoms: The Cisco 7600 crashes in a very rare case.

  Conditions: This symptom is observed very rarely when route-churn/sessions come up.

  Workaround: There is no workaround.

- CSCtk18404

  Symptoms: Per-user route is not installed after IPCP renegotiation.

Conditions: The symptom is observed with the following conditions:

1. PPP session comes up, NAS installs static routes which are sent as attribute from RADIUS server.
2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated but the static routes are lost.

Workaround: There is no workaround.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB and later. Earlier versions are not affected.

  Workaround: Advertise and withdraw or withdraw and re-advertise a more specific prefix. That will force the re-evaluation of the prefix not being imported, for import again.

- CSCtn67034

  Symptoms: The username attribute is missing in the accounting stop record even though the user is authenticated.

  Conditions: This symptom is observed when accounting is enabled for an unauthenticated session, and the start record does not have the username (as expected). After authenticating the session, the first accounting packet that goes out does not have the username, that is:

  1. The first interim packet, if interim is enabled.
  2. The stop record, if interim is not enabled or if the stop record is sent before the interim period expires.

  Workaround: Enable the interim so that the stop record will have the username information.

- CSCto16196

  Symptoms: Performing al **no wccp version2** on the WAAS device connected to the WAN link and then reconfiguring **wccp version 2** results in tracebacks on a Cisco ASR 1000 router configured with WCCP. Traffic loss is also observed.

  Conditions: This symptom is observed when WCCP is configured on a Cisco ASR 1000 router and the WCCP tunnels are up before **wccp version 2** is removed and reapplied on the WAAS devices.

  Workaround: There is no workaround.

- CSCto70633

  Symptoms: Packets get punted to the RP because the default ACL does not get programmed on the Distributed Feature line card (DFC), which causes high RP CPU.

  Conditions: This symptom is observed upon removal and reinsertion of the line card when there are VRF-scale configurations on the ES+ card as given below: More than 800 subinterfaces with VRF configurations

  Workaround: Reload the router.

- CSCto76700

  Symptoms: Multihop BFD session goes down with TE-FRR cutover.

  Conditions: The symptom may be observed with single hop, VCCV BFD and multihop BFD sessions. But after the TE-FRR cutover, the VCCV BF session comes back up whereas multihop BFD session goes down.

  Workaround: The workaround is to perform a “no shut” the port-channel interface.

- CSCto99343

  Symptoms: Linecards do not forward packets which causes a failure on the neighborship.

  Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.

  Workaround: There is no workaround.

- CSCtq08864

  Symptoms: Scalable EoMPLS VC imposition traffic drop.

  Conditions: This is seen with a scaled configuration of scalable EoMPLS VC with access facing as LACP etherchannel with dual member links spread across the ES40 NP modules. Upon flapping one of the member links followed by port- channel bundle flap, a random VC stops flowing traffic on the imposition side.

  Workaround: Trigger the reprogramming of the VC using **clear xconnect all**.

- CSCtq17082

  Symptoms: Router reloads.

  Conditions: The symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Virtual Template.

  Workaround: Session teardown before you remove the QoS configuration.

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: The symptom is observed after shutting down the link.

  Workaround: There is no workaround.

- CSCtq24614

  Symptoms: The commands to ignore S1 bytes are not supported on an ATM interface.

  Conditions: The symptom is observed with an ATM SPA.

  Workaround: There is no workaround.

- CSCtq58383

  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq80648

  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

  For example:

```
interface Ethernet1/0
  vrf forwarding vpn1
   ipv6 address 1::1/64
!
 router bgp 65000
  address-family ipv6 vrf vpn1
```

```
neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq82715

  Symptoms: When the VPLS VC goes up/down, the DHCP snooping LTL has not been updated, resulting in DHCP packet drop.

  Conditions: This symptom occurs when the VPLS VC goes up/down, indicating that the DHCP snooping LTL has not been updated.

  Workaround 1: Enable/disable snooping.

  Workaround 2: Clear the xconnect peer for the newly elected peer.

  Further Problem Description: In such an event, the GPI is now passed onto DHCP snooping code to program its LTL.

- CSCtq86515

  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.

  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.

  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- CSCtq91643

  Symptoms: Basic IP session with dot1q encapsulation and IP initiator may not come up.

  Conditions: The symptom is observed on an ES40.

  Workaround: Reconfigure the dot1q encapsulation (which has same VLAN ID as the outer VLAN ID of the QinQ subinterface) after an OIR.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr07704

  Symptoms: While using scripts to delete non-existent class map filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).

  Conditions: This symptom occurs when trying to delete a non-existent classmap filter, the classmap will be NULL, and passed to match_class_params_same. This results in referencing a null pointer.

  Workaround: Do null check in match_class_command and match_class_params_same. To keep existing behavior, do not print out a message like “the class does not exist” when deleting a non-existent class map from a class.

- CSCtr14675

  Symptoms: The line card crashes after removing the child policy in traffic.

  Conditions: This symptom occurs after the child policy is removed in traffic.

  Workaround: There is no workaround.

- CSCtr14852

  Symptoms: A Cisco 7600 router may experience the following error conditions:

  1. The router starts displaying ICC WATERMARK messages. (This is expected if it happens for a short duration and is not associated with the second symptom mentioned below).

     For example:

```
%ICC-SP-5-WATERMARK: 1375 multicast tx pkts for class L2-DRV(FC) are waiting to be
processed
-Traceback= 81757BC 85FB874 85FC09C 85E5684 85E7CC8 85F18DC 85F1C7C 85F2050 84436A4
8443EA4 835C958 8356C34
```

  2. The above symptom would trigger a situation where the flow control mechanism is turned "ON" by the communication infra (ICC). As a result, the communication infra will fail to carry application data from one point to another within the router. This in turn would lead to failure of multiple features that are dependent on the ICC.

     For example: The ICC flow control can be verified by the following command:

```
BFW01#sh icc flowcontrol
Class Name              FC state                    FC Counts (on/off)
                                          [ Local ]   [ Remote ]  [ IPC ]
=============================================================================
   37 EARL_NDE(FC)      [ OFF ]             0/0         0/0         0/0
   71 ACE_REQUESTS      [ OFF ]             0/0         0/0         0/0
   77 ICC_FC_TEST_REQU  [ OFF ]             0/0        0/0         0/0
   78 L3-MGR-QM(FC)     [ OFF ]             0/0         0/0         0/0
   79 L3-MGR-FM         [ OFF ]             0/0         0/0         0/0
   80 L3-MGR-INTF(FC)   [ OFF ]             1/0         0/0         0/0
```

  As shown above, the flow control is turned ON on L3-MGR-INTF, but never turned OFF.

  The ICC flow control mechanism is required to manage the ICC. If the flow control is turned on for a genuine reason, it will be turned OFF in a short while. This is expected.

  However, in this case, because of a bug in accounting, the flow control is turned ON (when not required), and never gets turned OFF, leading to the above situation.

Conditions: This symptom occurs during “ICC MULTICAST” (not IP multicast) usage. This issue may be caused by heavy route flaps or interface flaps.

Workaround: There is no workaround.

- CSCtr19286

  Symptoms: A “no shut” on an administratively down interface may result in overruns on other interfaces that are forwarding traffic. This occurs on ports being no shut for the first time in the same ASIC group. Subsequent shut/no shut on the same port does not cause this issue.

  Conditions: This symptom occurs under the following conditions:

  – This issue has been seen on Rohini ASIC-based DFC LAN cards such as WS-X6748-GE-TX.
  – The ports belong to the same port ASIC.
  – This issue is seen only the first time you no shut an interface

  Workaround: No shut all the ports in the ASIC group after bootup. Subsequent shut/no shut will not cause the overrun issue.

- CSCtr19922

  Symptoms: Lots of output printed by **show adjacency** *[key of adj] internal dependents* followed by a crash.

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

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

- CSCtr22007

  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

  Conditions: MPLS-TE Tunnel Flap.

  Workaround: There is no workaround.

- CSCtr27674

  Symptoms: A SIP-200 linecard crashes.

  Conditions: The symptom is observed with a POS SPA on SIP-200 linecard after performing an ISSU upgrade on a Cisco 7600 Series router.

  Workaround: There is no workaround.

- CSCtr28527

  Symptoms: After a few minutes of HA cutover, DHCP snooping on a VLAN stops.

  Conditions: This symptom occurs after a few minutes of HA cutover.

  Workaround: Shut/no shut the port-channel interface.

  Further Problem Description: After SSO, the LTL consistency checker starts recomputing fpoe for each LTL. For those from the sw-mcast region, the LTL cc makes a callback to retrieve the gpid list to program the fpoe for the LTL. In this case, the DHCP snooping feature provides an incomplete list because the VPLS VC programming is done directly by the cwan_atom code and the feature is unaware of this gpid list. The VPLS VC gpid programming to LTL is now redirected to the feature itself.

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

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

- CSCtr30621

  Symptoms: When working and protect LSPs are over different IMs, an OIR of one will bring down both.

  Conditions: The symptom is observed when you OIR the link for one LSP.

  Workaround: Shut/no shut the TP tunnel interface.

- CSCtr34793

  Symptoms: The router cannot establish mVPN PIM adjacencies over an MDT tunnel. The core PIM still works normally.

  Conditions: This symptom may occur after router reload when mVPN with PIM is configured and PIM-hellos from the neighbors are coming to the line card with DFC. Another possible trigger could be removal/recreation of the MDT in a VRF definition.

  Workaround: Reload the line card.

- CSCtr37073

  Symptoms: WS-X6196-RJ-21 and WS-X6148X2-RJ-45 may fail to come online on the Cisco 7600 router when running SRC or higher images.

  Conditions: This symptom occurs when SRC or higher images are run on a Cisco 7600 router.

  Workaround: There is no workaround.

  Further Problem Description: This issue occurs due to a timing problem in the module initialization routine of the Cisco IOS.

- CSCtr45608

  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

  Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- CSCtr45633

  Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.

  Conditions: The symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.

  Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address- family”.

- CSCtr51786

  Symptoms: The command **passive-interface** for a VNET auto- created subinterface x/y.z may remove the derived interface configuration command **ip ospf** *process id* **area** *number*. Consequently, putting back **no passive-interface** command will not form the lost OSPF ADJ.

  Conditions: The symptom is observed only with interfaces associated with the OSPF process using the command **ip ospf vnet area** *number*.

  Workaround: Associate the interface with the OSPF process using a network statement or using the interface command **ip ospf** *process id* **area** *number*.

  Further Problem Description: Interfaces associated with a process using a network statement under "router ospf" or interfaces configured with the command **ip ospf** *process id* **area** *number* are not affected.

- CSCtr53118

  Symptoms: The command **show mls cef ip lookup** *prefix* and **show mls cef ipv6 lookup** *prefix* returns IPv4 FIB Miss and IPv6 FIB Miss errors respectively.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 15.1(3)S.

  Workaround: Use **show mls cef ip** *prefix* and **show mls cef ipv6** *prefix* instead.

- CSCtr53677

  Symptoms: ARP failure is seen with the following **show** command:

  show arp vrf *vrf name*

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the ARP failure on the Gigabit subinterface.

  Workaround: There is no workaround.

- CSCtr53739

  Symptoms: The tunnel-encap entry is wrongly programmed. The following **show** command is used:

  show platform software multicast ip cmfib vrf *vrf- name* **tunnel-encap verbose**

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the tunnel-encap entry wrong programmed on the SP, with corrupt values.

  Workaround: There is no workaround.

- CSCtr69937

  Symptoms: The POS link flap in the core breaks the IPv4 PIC Core functionality.

  Conditions: This symptom occurs on Cisco 7600 routers running Cisco IOS Release 15.1(03)S.

  Workaround: Execute the **clear ip route** command for the affected prefix.

- CSCtr74529

  Symptoms: The following error messages are displayed:

  ```
  %ENVM-DFC3-4-LONGBUSYREAD: C2W Interface busy for long time reading temperature sensor
  1 %ENVM-DFC2-4-LONGBUSYREAD: C2W Interface busy for long time reading temperature
  sensor 2
  ```

  Conditions: This symptom is not caused by any specific conditions.

  Workaround: There is no workaround.

- CSCtr80366

  Symptoms: Relay miscalculates the giaddr from the OFFER packet, and hence cannot find the binding.

  Conditions: This symptom occurs while configuring multiple pools on the server and multiple secondary IP addresses on the relay loopback IP address.

  Workaround: There is no workaround.

- CSCtr89882

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

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

  Workaround: There is no workaround.

- CSCtr92067

  Symptoms: A Cisco 7609 that is running Cisco IOS Release 15.1(2)S1 may have CHUNKSIBLINGSEXCEED messages in the log/syslog. The following maybe seen from the supervisor:

  ```
  %SYS-SP-STDBY-4-CHUNKSIBLINGSEXCEED: Number of siblings in a chunk has gone above the
  threshold. Threshold:10000 Sibling-Count:12036 Chunk:0x1DC6D820 Name:Const IPv6 ADJ
  -Process= "Const2 IPv6 Process", ipl= 5, pid= 435 -Traceback= <snip>
  ```

  Or from a linecard:

  ```
  %SYS-DFC9-4-CHUNKSIBLINGSEXCEED: Number of siblings in a chunk has gone above the
  threshold. Threshold:10000 Sibling-Count:12008 Chunk:0x29B01260 Name:Const IPv6 ADJ
  -Process= "Const2 IPv6 Process", ipl= 5, pid= 303 -Traceback= <snip>
  ```

  Conditions: The symptom is observed on a Cisco 7609 that is running Cisco IOS Release 15.1(2)S1.

  Workaround: There is no workaround.

- CSCts15072

  Symptoms: Multicast traffic in the MVPN solution is dropped.

  Conditions: This symptom is observed on the Cisco 7600 series routers after deletion and (re)creation of a VRF.

  Workaround: Do not delete VRFs. All configuration related to a VRF can safely be removed. Only the VRF name should be retained in the configuration.

- CSCts39240

  Symptoms: The **advertise** command is not available in BGP peer-policy templates.

Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.

Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- CSCts39535

  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

  Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

  Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

  Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

  Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts47605

  Symptoms: For ECMP on the Cisco ASR1k router, RSVP does not select the right outgoing interface.

  Conditions: This symptom is observed with RSVP configuration with ECMP.

  Workaround: There is no workaround.

- CSCts51980

  Symptoms: STM1-SMI PAs of version 3.0 do not come up.

  Conditions: This symptom is observed when the new version of PAs do not come up with enhanced flexwan.

  Workaround: There is no workaround. Without the PA, flexwan will come up.

- CSCts67423

  Symptoms: On the Cisco ASR1k and ISR G2 only, call failures occur in the CUBE enterprise with interoperability to third-party SIP devices due to a trailing comma in the Server and User-Agent fields. For example:

  User-Agent: Cisco-SIPGateway/IOS-15.1(3)S,

  Server: Cisco-SIPGateway/IOS-15.1(3)S,

  You might see this with Cisco IOS Release 15.2(1)T or other versions. If the trailing comma is present it can cause interoperability issues. If there is no trailing comma, then this defect is not applicable.

  Conditions: This symptom is observed when there is an interoperability problem between the CUBE enterprise and a third-party SIP device. The trailing comma is invalid against RFC 2616 and the third-party SIP device ignores SIP messages from the CUBE.

Workaround: On both inbound and outbound dial peers, apply a SIP profile similar to the one below, or add the four lines to an existing SIP profile in use.

```
voice class sip-profile 1
 request ANY sip-header User-Agent modify "-15.*," ""
 response ANY sip-header User-Agent modify "-15.*," ""
 request ANY sip-header Server modify "-15.*," ""
 response ANY sip-header Server modify "-15.*," ""

dial-peer voice 1 voip
 voice-class sip profiles 1
```

Resolved Caveats—Cisco IOS Release 15.1(3)S0a

Cisco IOS Release 15.1(3)S0a is a rebuild release for Cisco IOS Release 15.1(3)S. The caveats in this section are resolved in Cisco IOS Release 15.1(3)S0a but may be open in previous Cisco IOS releases.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when “bgp deterministic-med” is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

Open Caveats—Cisco IOS Release 15.1(3)S

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

- CSCto16377

  Symptoms: DPD deletes only IPSec SAs. It does not delete IKE SAs.

  Conditions: This issue is observed when DPD is enabled and the peer is down.

Workaround: There is no workaround.

- CSCto45782

  Symptoms: When a tunnel interface in a DMVPN environment flaps, about 10 percent of the original number of tunnels do not get re-established automatically.

  Conditions: This issue is observed when all the following conditions are met:

  - RP2 and ESP20 are installed on the router.
  - The DMVPN hub has a large number (for example, 4000) of spokes connected to traffic.
  - IKEv1 and EIGRP are configured on the DMVPN hub.

  Workaround: Re-establish the tunnels by manually clearing them using the **clear crypto sa peer** command or the **clear crypto isakmp** command.

- CSCto56161

  Symptoms: Memory leaks are observed when 8000 ISGv6 PPP sessions out of 32000 ISGv6 PPP sessions with three TCs where one TC starts flapping.

  Conditions: This issue is observed when ISGv6 PPP sessions start flapping.

  Workaround: Reload the router.

- CSCto91593

  Symptoms: A packet loss is seen after an RPSO.

  Conditions: This issue is observed after an RPSO.

  Workaround: Run the **ip multicast redundancy routeflush maxtime** *300* command.

  There is no workaround.

- CSCtq08864

  Symptoms: Scalable EoMPLS VC imposition traffic drops.

  Conditions: This symptom is seen with scaled configuration of scalable EoMPLS VC with access facing as LACP EtherChannel with dual member links spread across the ES40 NP modules. Upon flapping one of the member links followed by port-channel bundle flap, some random VC stops flowing traffic in imposition side.

  Workaround: Trigger the reprogramming of the VC by using the **clear xconnect all** command.

- CSCtq14556

  Symptoms: If the active channel flaps while the standby channel is down, the multilinks do not come up.

  Conditions: This issue is observed if the active channel flaps while the standby channel is down. The MLP bundles remain inactive because the interfaces are down due to the LRDI error.

  Workaround: Bring up the standby channel.

- CSCtq15058

  Symptoms: A policy does not get attached to the LC after the policy map is modified and an OIR is performed.

  Conditions: This issue is observed after the policy map is modified and an OIR is performed.

  Workaround: There is no workaround.

- CSCtq17082

  Symptoms: Crash is observed with VTEMPLATE Background Manager when removing QoS configurations from Virtual-Template.

  Conditions: This scale issue happens with at least 2000 IPSec tunnel sessions by automatic script to remove QoS configuration from Virtual-Template.

  Workaround: There is no workaround.

- CSCtq31954

  Symptoms: High CPU utilization is observed during the AAA per-user process.

  Conditions: This issue is observed when there is a large number (for example, 15000) of TAL sessions.

  Workaround: There is no workaround.

- CSCtq40115

  Symptoms: Offset-list is not incrementing the metric by the correct value in EIGRP classic mode.

  Conditions: This symptom is seen only in classic mode and not in named mode.

  Workaround: Use EIGRP in named mode.

  Further Problem Description: When using offset-list in classic mode, the metric does not increase at all for small values like 10 or 20. For larger values, the metric increases by some random smaller value with no relation.

  This issue is not seen in EIGRP named mode since EIGRP named mode supports wide metrics.

- CSCtq56659

  Symptoms: Incorrect LC programming is seen with CEM interface.

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

  Workaround: Soft OIR.

- CSCtq57630

  Symptoms: Packets are lost due to high CPU utilization that occurs when a large number of data MDTs are configured at the same time.

  Conditions: This issue is observed when a large number of data MDTs are configured at the same time.

  Workaround: Configure a small number of data MDTs at a time.

- CSCtq67680

  Symptoms: When the SPA reloads, the event triggers a silent reload of the LC.

  Conditions: This issue is observed when a QoS policy is applied on the multilink bundle of the serial SPA.

  Workaround: There is no workaround.

- CSCtq67717

  Symptoms: Standby SUP is getting reset due to RF Client: IOS Config ARCHIVE after SSO while sync is happening.

  Conditions: This symptom occurs when archive is configured and performing SSO.

  Workaround: There is no workaround.

- CSCtq71477

  Symptoms: The **redistribute connected metric** *20000000 2 255 255 1500* command sets a bandwidth of 4294967295 Kbit.

  Workaround: There is no workaround.

  Further Problem Description: the **redistribute connected metric** *20000000 2 255 255 1500* sets a bandwidth of 4294967295 Kbit. All bandwidth values above 10000001 show the same value of 4294967295.

- CSCtq74691

  Symptoms: A buffer leak is observed at radius_getbuffer.

  Conditions: This symptom is observed when a DHCP request is initiated from the client. A DHCP address is allocated from the server, and a session comes up in the authentication state. A buffer leak occurs at radius_getbuffer and may increase with each new session.

  Workaround: There is no workaround.

- CSCtq79350

  Symptoms: Rekey fails in the GM after the ACL is changed in the key server a few times.

  Conditions: This issue is observed after the ACL is added to or removed from the key server.

  Workaround: Use the **clear crypto gdoi** command.

- CSCtq80074

  Symptoms: A router crashes when the **no ip trigger-authentication timeout** *90* **port** *1* command is executed.

  Conditions: This symptom is seen under the following conditions:

  – Configure “ip trigger-authentication timeout 90 port 1”

  – Configure “ethernet mac-tunnel virtual 4094”

  – Execute **no ip trigger-authentication timeout** *90* **port** *1* command.

  Workaround: There is no workaround.

- CSCtq80351

  Symptoms: SP crashes during a switchover in RPR mode.

  Conditions: This symptom is observed after the following failures and tracebacks with mcast scale configurations:

```
%SYS-SP-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from 0x82148C4,
alignment 32
Pool: I/O  Free: 2064  Cause: Memory fragmentation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
 -Process= "Pool Manager", ipl= 0, pid= 8
-Traceback= 81BA4D8z 8345490z 834ACB0z 82148C8z 835FC38z 835FF9Cz 83A301Cz 839D288z
CMD: 'sh redundancy state |  inc peer state' 18:21:22 IST Tue Jun 7 2011
Jun  7 18:21:22.575 IST: %SYS-SP-3-CPUHOG: Task is running for (2000)msecs, more than
(2000)msecs (27/2),process = SP Error Detection Process.
-Traceback= 0x8367AACz 0x821E7BCz 0x821EA94z 0x8E01830z 0x8BDDD60z 0x8E01A08z
0x96ED980z 0x96EBB34z 0x83A301Cz 0x839D288z
```

  Workaround: There is no workaround.

- CSCtq88437

  Symptoms: An IKEv2 memory leak results in RP reload. The memory leak speed depends on the session scale numbers. Session flapping will increase the leak.

  Conditions: This symptom is observed when tested with 4000 crypto map.

  Workaround: There is no workaround.

- CSCtq95291

  Symptoms: The router crashes.

  Conditions: This issue is observed when the saved configuration is copied to the startup configuration.

  Workaround: There is no workaround.

- CSCtq95873

  Symptoms: Some IPSec tunnels (DMVPN spokes) fail after the first IKE rekey.

  Conditions: This issue is observed when all the following conditions are met:

  - RP2 and ESP20 are installed on the router.
  - The DMVPN hub has a large number (for example, 4000) of spokes connected to traffic.
  - IKEv1 and EIGRP are configured on the DMVPN hub.

  Workaround: Reduce the number of tunnels (spokes) to 2000 or a smaller number.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when “bgp deterministic-med” is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr01431

  Symptoms: An error is encountered during configuration synchronization.

  Conditions: This issue is observed when the following sequence of steps is performed:

  1. A loopback interface is created
  2. The macro interface range is configured for the loopback interface.
  3. The loopback interface is deleted.

4. SSO is performed.

Workaround: There is no workaround.

- CSCtr06338

  Symptoms: IDSM2 service module does not come up.

  Conditions: This symptom occurs when IDSM2 service module heavy variant with RSP720-10GE.

  Workaround: There is no workaround.

- CSCtr12618

  Symptoms: With crypto map configured on a Cisco ASR 1000 series router with asr1000rp1-advipservicesk9.03.02.00.S.151-1.S.bin, if the crypto map ACL is changed, all IPSec traffic stops forwarding until tunnels rekey.

  Conditions: This symptom is seen in Cisco IOS Release 15.1(1)S.

  Workaround: Use the **clear crypto session** command to get crypto traffic to forward.

- CSCtr14867

  Symptoms: Static VTI tunnels terminating on a Cisco ASR 1000 series router that is using NAT-T due to a NAT rule in between the endpoints will fail to decapsulate traffic. The tunnel will build phase 1 and phase 2, the remote peer will show IPsec encaps and decaps, but the Cisco ASR 1000 series router will only show encaps with no decaps. This causes one-way outgoing traffic from the Cisco ASR 1000 series router side of the tunnel.

```
ASR1000#sh cry ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.12.1
protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer 192.168.15.1 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1008, #pkts encrypt: 1008, #pkts digest: 1008
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

The Drop reason from the ASR is IpsecInput.

ASR1000#show platform hardware qfp active statistics drop all
-----------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
-----------------------------------------------------------------------------
IpsecDenyDrop                                  0                      0
IpsecIkeIndicate                               0                      0
IpsecInput                                  1228                 233320
IpsecInvalidSa                                 0                      0
IpsecOutput                                    0                      0
IpsecTailDrop                                  0                      0
IpsecTedIndicate                               0                      0
```

Conditions: This symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release XE 3.3.1S with NAT-T tunnels using udp/4500 for encrypted traffic and static VTIs are in use.

Workaround: Remove NAT and use ESP for encapsulating encrypted packets. Downgrade to Cisco IOS Release 15.1(2)S. Use dynamic VTIs.

Resolved Caveats—Cisco IOS Release 15.1(3)S

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

- CSCsd55997

  Symptoms: When the **archive tar/xtract tftp://***TFTP_ADDRESS***/tarball.tar flash:** command is used to unpack the contents of a TAR file to the flash: filesystem, the extraction process may cease right after the first “large file” is unpacked. All files in the TAR file which follow this “large file” will not be unpacked.

  Conditions: This behavior may be observed on Cisco IOS router platforms where the target flash: filesystem is Class B (LEFS). The source path of the TAR file may be TFTP or FTP. All Cisco IOS releases are affected.

  There is no problem unpacking all the contents of the TAR file when the target flash: filesystem is Class C (DOSFS).

  Workarounds:

  1. If possible format the target flash: filesystem as DOSFS (**format flash:**) as opposed to LEFS (**erase flash:**).
  2. If there is a second target media available (say slot0:), copy the TAR file there first and then unpack the TAR file to flash: **archive tar/xtract slot0:tarball.tar flash:**.
  3. If you are preparing your own TAR files, order all the “large files” at the end of the TAR file, with the largest “large file” as the last file in the archive.

- CSCsl74976

  Symptoms: When MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled. No packets are processed from throttled interfaces (until interface is unthrottled). If control plane protocols are running on throttled interfaces (especially with aggressive short timeouts), frequent throttling can lead to instabilities (such as BGP session loss, OSPF adjacency flaps, HSRP failovers, BFD neighbor less, etc.).

  Conditions: This symptom occurs when MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled.

  Workaround: A certain level of stability can be gained by increasing hold queues on interfaces in questions. Also reducing the rates and duration of the traffic punting to MSFC CPU will help.

- CSCsx64858

  Symptoms: A router may crash after the **show ip cef vrf** *VRF* **platform** command is issued.

  Conditions: This symptom occurs when BGP routes are learned via two equal paths within a VRF. If an update occurs so that only one path remains while the **show ip cef vrf** *VRF* **platform** command is issued, the router may crash.

  Workaround: There is no workaround.

- CSCsz53809

  Symptoms: There is an infinite reload of a VSS member due to configuration mismatch between peers.

  Conditions: This symptom is due to the use of double quotes in VLAN name configuration, which causes the rejection of that name during the initialization of a member after its reload.

  Workaround: There is no workaround.

- CSCta10402

  Symptoms: Continuous packet send by BFD causes a CPU hog.

  Conditions: The symptom is observed when BFD is enabled in the router.

  Workaround: Disable BFD.

- 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.

- CSCtf39056

  Symptoms: RRI route will not be deleted even after IPSec SA has been deleted.

  Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
############
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry  "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
############
```

- 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.

- CSCti10828

  Symptoms: In Cisco IOS Release 12.4T, there is no response to SNMP queries of:

  ```
  1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive
  1.3.6.1.4.1.9.9.276.1.1.2.1.12 cieIfHighSpeedReceive
  ```

  within the CISCO-IF-EXTENSION-MIB although supported at the CLI:

  ```
  interface GigabitEthernet0/3
   bandwidth receive 100 <<<<<

  ==> , BW 100000 Kbit/sec, RxBW 100 Kbit/sec
  ```

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCti48483

  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.

- CSCti16649

  Symptoms: GETVPN GM reregisters.

  Conditions: This symptom is seen when any ACL is added or removed from the key server.

  Workaround: There is no workaround.

- CSCti23324

  Symptoms: With some L2 DEC configurations, recirculation may be added during packet forwarding.

  Conditions: This symptom is seen with L2 DEC and PFC3B configurations.

  Workaround: This is not a forwarding issue. Remove L2 DEC or use PFC3C in the L2 DEC.

- CSCti87194

  Symptoms: The last fragment causes a crash because of an invalid zone value.

  Conditions: This symptom occurs when a Big IPC message is fragmented. Then, the last fragment causes the crash because of an invalid zone value.

  Workaround: There is no workaround.

- CSCti98219

  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.

- CSCtj04672

  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.

- CSCtj14921

  Symptoms: During the stress test of EzVPN, many messages are observed on the console like the following:

  ```
  "%PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled interrupt for 11 msec"
  ```

  The EzVPN server is configured for dVTI and dynamic crypto maps. The stress test consists of bringing up and tearing down close to 1700 EzVPN clients (1250 dVTI and 450 dynamic cmap) clients.

  Conditions: This symptom is seen on a Cisco ASR 1006 router with RP2/FP20 combo with EzVPN clients coming in on GigE interfaces and on the latest XE3.2 throttle build. Many messages are seen on the console followed by tracebacks.

  Workaround: There is no workaround.

- CSCtj65692

  Symptoms: The service policy applied to a service instance stops forwarding any traffic. The output of the **show policy-map interface** *x/y* command indicates that all packets are hitting the violation queue. The conform counter does not increase at all and all traffic is dropped.

  Conditions: This symptom is observed in Cisco 7600 with policers/LLQ on ES+ interfaces. This issue is applicable for the service policy (policing or LLQ) applied for ingress or egress traffic.

  Workaround: There is no workaround.

  Removing and reapplying service-policy may clear the condition for temporarily, but it can reappear. The issue is specific to policers. If possible, shapers can be used instead of policers to avoid the issue.

- CSCtj84234

  Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

route-map *RM name*

match ip address *acl*

set ip next-hop *NH1 NH2*

Workaround: There is no workaround.

- 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.

- CSCtj94589

  Symptoms: With the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF and four SA dual per session, in unconfigured testbed after end of the IXIA traffic, crash happens at "no vrf" under "crypto isakmp profile".

  Conditions: This symptom is seen with the configuration of 1000 VRFs (fvrf! =ivrf), with one IKE session per VRF and four SA dual per session.

  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.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  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-ipsla.shtml.

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to re-sync after the server clock changes its time and after the NTP falls back to the local clock.

  Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

  Workaround: There is no workaround.

- CSCtk99699

  Symptoms: Rekey functionality is broken if you remove and add crypto key again.

  Conditions: This symptom occurs when removing the key and adding again. The rekey is not working.

Workaround: Use the **clear crypto gdoi** command.

- CSCtl49917

  Symptoms: Minor diagnostic error is seen on SIP-400.

  Conditions: This symptom occurs when scaled configurations are applied to ES+ and SIP-400. The BusConnectivity test fails on SIP-400 during boot-up.

  Workaround: Power enable SIP-400 after all the line cards have come up in the test bed. Or, after a couple of retries, reload SIP-400, and it automatically comes up.

- CSCtl90292

  Symptoms: The following error messages are displayed:

  ```
  an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes
  failed from 0x42446470, alignment 32
  Pool: I/O  Free: 11331600  Cause: Memory fragmentation Alternate Pool: None
  Free: 0  Cause: No Alternate pool  -Process= "BGP I/O", ipl= 0, pid= 564
   -Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
  40FD1964 403BDBFC 403BCC34 40344508 403668AC
  ```

  Conditions: This symptom is observed when several hits and failures are seen for medium buffers. All are linktype IPC. For example:

  ```
  Buffer information for Medium buffer at 0x4660E964
  ...
    linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
    if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)
  ```

  Workaround: There is no workaround.

- CSCtl90570

  Symptoms: PIM neighborship is lost on one of the PEs (source node).

  Conditions: This symptom occurs when reloading all the routers simultaneously.

  Workaround: Use the **clear mpls mldp neighbor *** command.

- CSCtn22961

  Symptoms: With the pseudowire redundancy, after performing “clear xconnect all” on the remote primary peer, the VCs that switchover to the backup PWs are now in the standby state on the primary peer. However, they are in down state on the local node instead of standby state.

  Conditions: This symptom occurs when performing “clear xconnect all” on the remote primary peer where initially all the VCs are in UP state.

  Workaround: There is no workaround.

- CSCtn36227

  Symptoms: Alignment errors are seen at ipv6_checksum.

  Conditions: This symptom is seen when the GRE tunnel is configured with IPv6 ping sweep going across.

  Workaround: There is no workaround.

- CSCtn51058

  Symptoms: Traffic drops cause long multicast reconvergence times.

  Conditions: This symptom occurs when performing Stateful Switchover (SSO).

Workaround: There is no workaround.

- CSCtn52270

  Symptoms: CWMP is not coming up.

  Conditions: This symptom is seen because of the “alcdsl_get_wan_dsl_link_config” function.

  Workaround: There is no workaround.

- CSCtn55847

  Symptoms: A memory leak is seen in crypto IKMP.

  Conditions: This symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(1)S2 that is acting as an IPSEC Hub based on DVTI. This happens when IPSEC spokes are flapping.

  Workaround: There is no workaround.

- CSCtn61834

  Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.

  Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keep alive message is received.

  Workaround: There is no workaround.

- CSCtn62287

  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

  Workaround: There is no workaround.

- CSCtn64879

  Symptoms: After configuring service group, traffic will go through both of the memberlinks of Ethernet Virtual Connection (EVC) point of contact (PoC) with xconnect.

  Conditions: This symptom is seen when defaulting the PoC configuration and adding it back.

  Workaround: Reset line card.

- CSCtn67577

  Symptoms: SIP-400 crashes while modifying the cell-packing values.

  Conditions: This symptom occurs when cell-packing values are modified at PE2 side.

  Workaround: There is no workaround.

- CSCtn67637

  Symptoms: Traffic is not forwarded from the DECAP PE in the egress replication mode.

  Conditions: This symptom occurs when the ingress LC on the DECAP PE is a CFC LC like 6748/SIP400 and the egress replication mode is used on the DECAP PE in a mVPN setup.

  Workaround: Switch to the ingress replication mode on the DECAP PE. Then, the traffic will start flowing.

- CSCtn68643

  Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

  Conditions: This symptom occurs when configuring OSPFv3 IPSec authentication or encryption.

```
ipv6 ospf encryption ipsec spi 500 esp null sha1
12341234123412341234123412341234123412341234
```

or

```
ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
```

Workaround: There is no workaround.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCtn95344

  Symptoms: After RPR downgrade from SRE2 CCO to SRE1 CCO, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.

  Conditions: This symptom occurs after RPR downgrade from SRE2 CCO to SRE1 CCO.

  Workaround: Perform reload on the router.

- 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.

- CSCtn99858

  Symptoms: Crashinfo is seen.

  Conditions: This symptom is observed during an 8k session.

  Workaround: There is no workaround.

- CSCto00318

  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

  For now, consider not initiating a SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

  Workaround: There is no workaround.

- CSCto07919

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

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

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- CSCto09059

  Symptoms: CPUHOG at IPC Check Queue Time Process results in IOSD crash.

  Conditions: This symptom occurs with multiple RP switchovers with ISG PPPoE sessions.

  Workaround: There is no workaround.

- CSCto10336

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

  Conditions: This symptom occurs during control channel cleanup.

  Workaround: There is no workaround. This symptom can be only removed through power cycle.

- CSCto11025

  Symptoms: When traffic streams are classified into multiple classes included with LLQ with qos-preclassify on the tunnel interface and the crypto map applied to an interface, packets are dropped on crypto engine on the Cisco 890 series router with buffers unavailable.

  Conditions: This symptom is observed when IPSec and QoS are used when qos-preclassify is on the tunnel interface and a crypto map is on the main interface.

  Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- CSCto11957

  Symptoms: PPPoE is terminated on port-channel with ES+ session limit error occurring incorrectly.

```
%CWAN_RP-6-SESS_LIMITS_PORT_GROUP: Exceeded max number of sessions supported
on
port-group
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[ADJ:PPPoE:5789] - hardware platform error.

Mismatch in sessions on RP and ES+:
BRAS#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                TOTAL     PTA   FWDED   TRANS
TOTAL                              57      56       0       1
Port-channel100                    57      56       0       1

BRAS#show platform isg session-count 4
 ES+ line card
 Sessions on a port-channel are instantiated on all member ports
 Port-group          Sess-instance   Max Sess-instance
 ----------          -------------   -----------------
 Gig4/11-Gig4/15              2936                4000 <<<<<<< INCORRECT
```

Conditions: This symptom is seen when scaled PPPoE sessions are terminated on port-channel with ES+ ports. Sessions negotiate, disconnect and attempt to renegotiate port-channel number other than port-channel 2.

Workaround: Change port-channel number to port-channel 2. Configure sessions to terminate on stand-alone ports.

- CSCto15278

  Symptoms: Tracebacks are seen at managed_chunk_low.

  Conditions: This symptom occurs when sending multicast traffic and using the **show memory debug leaks chunks** command.

  Workaround: There is no workaround.

- CSCto29720

  Symptoms: Packets drop in the LLQ queue without any congestion on the link when the line card is SIP-400.

  Conditions: This symptom occurs when LLQ is configured under Shaper on the physical interface and the line card is SIP-400.

  Workaround: There is no workaround.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.

  A **show process memory sorted** command may initially show “MallocLite” growing. By disabling malloclite with the following:

  ```
  config t
  no memory lite
  end
  ```

  One may start to see process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80mb per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on affected router, if possible.

- CSCto50255

  Symptoms: Memory leak occurs while running UDP echo operation.

  Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory** *pid* command.

  Workaround: There is no workaround.

- CSCto53332

  Symptoms: A router configured for IPSEC accounting may display the following error message:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  This does not seem to result in any impact apart from intermittently lost accounting messages.

  Conditions: This symptom occurs when ipsec accounting is active.

  Workaround: There is no workaround.

- CSCto55567

  Symptoms: The ES+ card goes to a major error state because of fabric CRC errors.

  Conditions: This symptom occurs after SSO with multicast traffic flowing through the line card.

  Workaround: Soft reload the line card.

- CSCto55606

  Symptoms: When same remote unicast neighbor is configured and received on different interfaces, the two neighbors keep flapping.

  Conditions: This symptom is seen when the same EIGRP neighbor is coming up on different interfaces.

  Workaround: This may not be a recommended configuration since having the same neighbor on different interfaces is not allowed in classic mode. This option is provided only for certain migration scenarios.

- CSCto55708

  Symptoms: There is a build error due to a missing “ " “ in a printf statement, only in dsgs, due to compiler-specific issues.

  Conditions: This symptom occurs due to a missing “ " “ in a printf statement only in dsgs due to compiler-specific issues.

  Workaround: There is no workaround.

- CSCto55812

  Symptoms: The router may crash.

  Conditions: This symptom occurs on entering vlan mode from a different mode, for example vfi, without exiting from the previous command mode.

  Workaround: Always exit from the current command mode while entering into another command mode.

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCto60216

  Symptoms: Cisco IOS crashes in ospfv3_write.

  Conditions: This symptom occurs when the **issu runversion** command is entered multiple times within a short period of time.

  Workaround: Wait for the newly active router processor to completely initialize.

- CSCto61485

  Symptoms: High CPU utilization is seen after session disconnect.

  Conditions: This symptom is observed with scaling test cases with 10K to 24K sessions.

  Workaround: There is no workaround.

- CSCto63720

  Symptoms: No traffic passes after a link flap if port-security is configured on the Gigabit Ethernet interface on 6748 LC.

  Conditions: This symptom occurs when the Cisco IOS version running is Cisco IOS Release 12.2(33)SRE2. This issue is seen when port-security is configured on a 6748 port and the link flap occurs on this interface.

  Workaround: Reconfiguring port-security fixes the problem.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

  Conditions: This symptom is seen with GETVPN related configurations with fail-close feature activated.

  Workaround: There is no workaround.

- CSCto70972

  Symptoms: Multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Conditions: This symptom occurs when multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Workaround: There is no workaround.

- CSCto71075

  Symptoms: High CPU usage is seen on changing root node multiple times in an MLDP setup. Loss of pim neighborship is also seen when changing path in a P2MP setup.

  Conditions: This symptom occurs when ptcam redirection being enabled for Lspvif can cause unexpected results. By default, Lspvif ptcam redirection is disabled. This fix ensures that this is taken care of in scenarios of pim state change.

  Workaround: There is no workaround.

- CSCto74038

  Symptoms: After an upgrade to SRE3, the CESoPSN (clock) pseudowire stays down due to payload size value mismatch.

  Conditions: This symptom occurs when, before the upgrade to SRE3, the payload size is configured to 80 and dejitter value is the default (5). After the upgrade, the payload size 80 and dejitter 5 combination is not accepted anymore as it is not the recommended value, so the payload size is removed from the configuration. The pseudowire is therefore configured with the default payload size. The default value is not accepted by the remote end of the pseudowire, thus leading to payload size mismatch.

  Workaround: Configure an acceptable dejitter value, and then reconfigure the payload size.

- CSCto76009

  Symptoms: Crypto SS crashes on DVTI server after using the **clear crypto session** command on DVTI client after all SAs have been established.

  Conditions: This symptom occurs when sessions are set up with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session.

  Workaround: There is no workaround.

- CSCto77225

  Symptoms: The states for VCs with MTP configurations remain up and on standby on standby POA.

Conditions: This symptom is seen when SSO is followed by a pmLACP/mLACP switchover.

Workaround: There is no workaround.

- CSCto77233

  Symptoms: The supervisor module on the Cisco 7600 router resets.

  Conditions: This symptom is observed when you use the **show ip cef** *prefix* platform internal command on the SP CPU and let it allow to hang on the --more-- prompt for long. When the underlying data gets changed or cleaned up due to waiting for long on --more-- prompt, the CLI can end up referencing wrong data resulting in router reset.

  Workaround: There is no workaround.

- CSCto77352

  Symptoms: Standby cannot reach HOT sync state with active. Standby RP will keep resetting. The following messages are printed:

  ```
  %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1),process
  = IPC Dynamic Cache.
  ```

  Conditions: This symptom occurs with SSO mode when a Cisco ASR 1000 series router is configured with ISG as DHCP server and with low DHCP lease timer.

  Workaround: There is no workaround.

- CSCto77504

  Symptoms: With shape configured on port-shaper and bandwidth-percent configured on groups in the EVC, on dynamic configuration of port-shaper value, the groups do not get the updated shape values based on bandwidth percent.

  Conditions: This symptom is seen when bandwidth-percent is configured on group or EVC with port-shaper.

  Workaround: There is no workaround.

- CSCto79174

  Symptoms: A Cisco 7600 router crashes with the following logs:

  ```
  Frames of RPC pm-cp process (pid 325) on 6 (proc|slot) after blocking rpc
  call failed: 8331CD0 855F3F4 8546A58 85E3F98 85E4910 86009E4 86BF18C 86BC44C
  86BDE8C 8601090 8601394 835B498 8355774

  Failed to send card online to CP, slot 2

  %Software-forced reload


  Unexpected exception to CPU: vector 1500, PC = 0xAF8765C , LR
  = 0xAF87620
  ```

  Conditions: Conditions are not known.

  Workaround: There is no workaround.

- CSCto80714

  Symptoms: Prowler SPA goes out of service with heartbeat failures when traffic flows through the MLPPP (multilink) interface. This issue is seen only in the Cisco IOS Release 12.2SRE throttle and not in mcp_dev. Some optimizations and a microcode reload-related fix is also included as part of this DDTS.

  Conditions: This symptom is observed when traffic flows through the MLPPP interface on Prowler. Microcode and SPA reload is required to recover.

  Workaround: There is no workaround.

- CSCto81530

  Symptoms: Task hung errors are seen in hal_dist_commit from cmfi code.

  Conditions: This symptom occurs when mldp configurations are loaded in a scaled environment.

  Workaround: There is no workaround.

- CSCto88686

  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.

- CSCto93880

  Symptoms: Enable authentication fails when user is configured with TACACS server group.

  Conditions: This symptom occurs when TACACS server is configured with user defined group and configured for enable authentication. User is unable to authenticate when he tries to switch to privilege executive mode (enable) and gets an error that indicates that there is no address for defined servers.

  %TAC+: no address for get_server

  %TAC+: no address for get_server

  Workaround: Configure the TACACS server group with the default group name.

- CSCto95591

  Symptoms: ES+ crash occurs.

  Conditions: This symptom is observed when vpls over the gre tunnel is configured and shut/no shut of the tunnel interface is done.

  Workaround: There is no workaround.

- CSCto99226

  Symptoms: Multicast packets are not forwarded.

  Conditions: This symptom occurs when the physical interface in the outgoing interface list (olist) of S,G has local join.

  Workaround: There is no workaround.

- CSCtq01136

  Symptoms: There is a ping failure over tunnel interface.

  Conditions: This symptom is seen during 6VPE basic configuration.

  Workaround: There is no workaround.

- CSCtq06105

  Symptoms: In an IP-FRR setup, after shut and unshut of the primary interface, traffic continues to flow along the backup interface, which is wrong. Traffic should flow along the primary path once the primary path is restored.

  Conditions: This symptom occurs with an IP-FRR setup. The primary interface should be shut and unshut to see the issue.

  Workaround: Shut and unshut the backup interface. This will reprogram the FRR, but this will cause a traffic drop.

- CSCtq09088

  Symptoms: The router crashes while trying to unconfigure “ip rsvp sender-host 10.0.0.5 10.0.0.1 UDP 11 11 10 10 identity bogusID”.

  Conditions: This symptom is observed on the Cisco 7200 router that is running the c7200-adventerprisek9-mz.122-33.3.13.SRE image.

  Workaround: There is no workaround.

- CSCtq09206

  Symptoms: Traffic flowing via MPLS TE tunnels gets blackholed after FRR-protected primary link flaps initiate an FRR cutover. CEF Backwalk failure messages may be observed on the SP/DFC console.

  Conditions: This symptom is observed with TE/FRR configuration with node protection.

  Workaround: There is no workaround.

- CSCtq10019

  Symptoms: After router reload, rate-limiters for multicast do not come into effect and packets are punted.

  Conditions: This symptom occurs during high CPU load when mfib is unable to distribute into lc and SP.

  Workaround: There is no workaround.

- CSCtq12230

  Symptoms: When overhead accounting command “hw-module slot 1 account np 0 out 4” is configured on the ES+ LC, show policy-map interface counters do not get updated.

  Conditions: This symptom is seen with QoS on any ES+ interface with overhead accounting feature enabled.

  Workaround: There is no workaround.

- CSCtq14829

  Symptoms: Traffic drops are seen in a DMVPN ph3 hierarchical setup. Traffic is flowing through spoke-hub-spoke path. Dynamic tunnel is not building between spokes.

  Conditions: This symptom occurs when traffic drops are seen at rhub1 when the number of tunnels is 50 or more.

  Workaround: There is no workaround.

- CSCtq21258

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

  Conditions: This symptom is seen when the user password is larger then 32 bytes and is being reduced to exactly 32 bytes.

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

- CSCtq21435

  Symptoms: Some specific s,g entries do not pass traffic with mldp during root node redundancy switchover.

  Conditions: This symptom occurs in case of mldp + RNR. This issue is seen when Accept Vlan is programmed as zero in the platform.

  Workaround: Clear the mroute.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS-XE Release 15.1(2) S may crash upon performing a CRL check on an invalid certificate.

  Conditions: The conditions are unknown.

  Workaround: Turning off CRL check should stop the crash. It should be configured as:

  “revocation-check none”

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq23038

  Symptoms: With “platform control-packets use-priority-q disable” configured on the port-channel main interface, after shut/no shut on the port-channel or member-link, port-channel subinterfaces do not inherit the “platform control-packets use-priority-q disable” feature.

  Conditions: This symptom occurs when you perform shut/no shut on a member-link or link flaps with port-channel subinterfaces and “platform control-packets use-priority-q disable” configured on the port-channel.

  Workaround: A possible workaround is to remove and reconfigure the subinterfaces.

- CSCtq23158

  Symptoms: The dlfi o atm fails to come up on sip400 with Cisco IOS Release 15.0(1)S images onwards if an ES+ card is present.

  Conditions: This symptom occurs when you cannot bring up dlfi o atm.

  Workaround: A possible workaround is to power down all ES+ cards.

- CSCtq23793

  Symptoms: After reloading PE router in mVPN network, multicast traffic stops on one of the VRFs randomly.

  Condition: This symptom occurs under the following conditions:

  -When reloading a PE in mVPN network. -When PE has many VRFs and scaled mVPN configuration.

Workaround: Remove and add MDT configuration.

- CSCtq29554

  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

  Workaround: Reload the failing line card to recover it.

- CSCtq30686

  Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.

  Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.

  Workaround: There is no workaround.

- CSCtq31338

  Symptoms: ESM20 crashes with MLDP intranet test.

  Conditions: This symptom occurs with access interface flapping a couple of times.

  Workaround: There is no workaround.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq33102

  Symptoms: A Cisco router that is acting as an RA crashes in an SDP environment with CVO setup.

  Conditions: This symptom occurs during CVO enrollment request.

  Workaround: There is no workaround.

- CSCtq34807

  Symptoms: Service group does not take effect on EVC Xconnect on a port channel.

  Conditions: This symptom is observed with a service group configuration on EVC Xconnect existing on a port channel. This issue is seen when EVC is removed and the configuration is reapplied.

  Workaround: Remove and reapply the service group.

- CSCtq36726

  Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual- access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

  Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

  Workaround: Reconfigure the Virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

- CSCtq37538

  Symptoms: Duplicate traffic is seen during route changes with p2mp te for multicast or mldp.

  Conditions: This symptom occurs during LSM configuration and route changes.

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

- CSCtq38303

  Symptoms: A policy is rejected with an insufficient bandwidth percent guarantee.

  Conditions: This symptom is observed with bandwidth percentage guarantees.

  Workaround: Do not configure bandwidth in percentages.

- CSCtq43480

  Symptoms: A Cisco router crashes.

  Conditions: This symptom occurs when a session starts with PBHK and accounting features while the method list is not provisioned for the accounting features.

  Workaround: There is no workaround.

- CSCtq50674

  Symptoms: Total traffic drop is seen for 6PE/6VPE when IPFRR is configured in the core.

  Conditions: This symptom occurs when BGP/6PE peer is protected by IPFRR in core.

  Workaround: There is no workaround.

- CSCtq52345

  Symptoms: IPv6 sessions sync to standby. IPv6 sessions are up on standby. After switchover the IPv6 sessions drop traffic.

  Conditions: This symptom is seen with switchover of IPv6 sessions.

  Workaround: Clear sessions and start reestablishment.

- CSCtq55723

  Symptoms: With Transport Control Protocol (TCP) and User Datagram Protocol (UDP), operations with VPN Routing and Forwarding (VRF) are not working.

  Conditions: This symptom occurs only with VRF.

  Workaround: Works without VRF.

- CSCtq56845

  Symptoms: Static PW over P2MP TE traffic might not pass through access facing SIP-400.

  Conditions: This symptom is seen with static PW with P2MP TE. On the SIP-400 drops are seen with MTU exceeded in “show plat drop detail” on the access facing SIP-400.

  Workaround: There is no workaround.

- CSCtq56948

  Symptoms: The default route attribute is used by features like uRPF and if it is missed out, it may cause uRPF to allow packets whose source addresses match against the default route.

  Conditions: This symptom occurs because some prefixes in the FIB are sourced by non-RIB features, such as CTS, or are used to represent next hops for recursive paths. Such prefixes inherit the forwarding information from their covers, but the default route attribute is not inherited.

  Workaround: There is no workaround.

- CSCtq57054

  Symptoms: ISSU between Cisco IOS Release XE 3.3.0S and Cisco IOS Release XE 3.4.0S is affected due to config sync issue.

  Conditions: A newly introduced CLI in Cisco IOS Release XE 3.4 is not phrased properly to support the backward compatibility.

  Workaround: There is no workaround.

- CSCtq59827

  Symptoms: MLDP and traffic are not passing at bud node.

  Conditions: This symptom is seen when MLDP/LSM and traffic are not passing at bud node. Some stale adjacencies will be seen for label entry programming in the hardware.

  Workaround: Remove the OIF and add it back. (Do a shut/no shut).

- CSCtq60383

  Symptoms: Traffic outage is observed after TEFRR cutover in an MLDP setup.

  Conditions: This symptom is observed when “mpls ldp explicit-null” is configured on all the provider boxes.

  Workaround: Unconfigure “mpls ldp explicit-null”.

- CSCtq62600

  Symptoms: Double LSM entries are seen.

  Conditions: This symptom is observed while changing the configurations from a same slot FRR to a different slot FRR.

  Workaround: Reload the router.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq63744

  Symptoms: MAC withdrawal is not sent to the core VCs on reception of STP TCN for MST.

  Conditions: This symptom is seen when access has switchport only.

  Workaround: There is no workaround.

- CSCtq67970

  Symptoms: Inter-AS IPv4 multicast streams do not resume if the source of the multicast stream is stopped. The s,g state expires in the transit AS, and traffic source is started again.

  Conditions: This symptom occurs when BGP PIC CORE/EDGE is configured in the system.

  Workaround: There is no workaround.

- CSCtq71011

  Symptoms: The router crashes, or in some cases a traceback is seen.

  Conditions: This symptom is seen when IPv6 routes with diverse paths are enabled.

Workaround: There is no workaround.

- CSCtq79767

  Symptoms: IPSEC key engine crashes after using the **clear crypto session** command on CES.

  Conditions: This symptom occurs under the following conditions:

  1. Topology:

     IXIA --> CES (DVTI Client) --> UUT (DVTI Server)-->

  2. Configuration:

     1000 vrf x 1 IKE session x 4 IPsec SA dual

  3. The crash on UUT is seen after using the **clear crypto session** command on CES after all SAs have been established.

  Workaround: There is no workaround.

- CSCtq80603

  Symptoms: Newly created SVIs are in down/down state.

  Conditions: This symptom occurs when SW VLAN RP process is stuck.

  Workaround: The following workarounds may work:

  1. Set the memory location of l2vlanifmib_access_count to zero after warm restart of snmp-sever.
  2. Perform SSO and/or LC OIR.
  3. Perform an active reload.

- CSCtq83677

  Symptoms: High traffic loss (around 15 sec) is seen for receivers on MVR receiver ports during SSO.

  Conditions: This symptom is seen during SSO.

  Workaround: There is no workaround.

- CSCtq85564

  Symptoms: The fix of CSCto77352 may cause a data corruption problem.

  Conditions: This symptom is seen when two processes are calling the same function that is raising the race condition.

  Workaround: There is no workaround.

- CSCtq86216

  Symptoms: Multicast traffic flows over both primary and backup interfaces during TEFRR reopt.

  Conditions: This symptom occurs when multicast traffic flows over an MLDP core with TEFRR link protection.

  Workaround: Duplicate traffic flows only for a short period of time (20 seconds). So, the issue gets automatically resolved after 20 seconds.

- CSCtq91305

  Symptoms: Standby cannot reach HOT sync state with active. The standby RP keeps resetting. The following message is displayed:

  ```
  %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1),process
  = IPC Dynamic Cache.
  ```

Conditions: This symptom occurs with SSO mode, when the Cisco ASR 1000 series router is configured with ISG as dhcp server and with a low dhcp lease timer.

Workaround: There is no workaround.

- CSCtq91403

  Symptoms: High CPU can be seen during reloads under the MVPN topology.

  Conditions: This symptom occurs in an MVPN network with an S,G with an incoming interface over the MDT tunnel, when there are no forwarding interfaces for that S,G.

  Workaround: A possible workaround is to create a static join for that S,G to protect the RP CPU. Also, in some case multicast rate-limiters will be useful.

- CSCtq92182

  Symptoms: An eBGP session will not be established.

  Conditions: This issue is seen when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq93823

  Symptoms: Ping drops with fragment size of 256.

  Conditions: This symptom occurs when doing a sweep ping with sizes 500 to 1000.

  Workaround: Flap the interfaces.

- CSCtq94418

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

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

  Workaround: Create dummy access subinterfaces belonging to a new vrf. Do not remove the interface.

- CSCtq97646

  Symptoms: A Cisco 7600 ES+ and SIP-400 card may crash when Dynamic Ethernet Services Activation (DESA) is configured, and certain attributes are downloaded from a radius server.

  Conditions: This symptom is seen when DESA is configured, and the radius profile that it downloads for an EVC contains an idle-timeout and dot1q range for the “stag-vlan-id” attribute. The card will crash.

  The ES+ card will crash as soon as the attributes are downloaded while a SIP- 400 may crash when the idle-timer expires.

  Radius Example:

```
simulator radius subscriber 25029
# [28] idle-timeout
 attribute 28 numeric 60
 vsa cisco generic 1 string "subscriber:sss-service=vpws"
 vsa cisco generic 1 string "l2vpn:service-
id=atom_from_agg22_to_dist2_int1_cfg1_1_of_1000"
 vsa cisco generic 1 string "l2vpn:redundancy-group=2"
 vsa cisco generic 1 string "ethernet-service-instance:service-instance-
```

```
description=... Dynamic EFP on Po2, stag:2000-2009, CFG_SEQ:1306963076"
 vsa cisco generic 1 string "l2vpn:redundancy-priority=2"
 vsa cisco generic 1 string "cdp:l2protocol-pdu-action=forward"
 vsa cisco generic 1 string "accounting-list=ACCT11"
 vsa cisco generic 1 string "ethernet-service-instance:stag-vlan-id=2000-
2009"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress=1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-tag-
operation=Push1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
type=0x8100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
vlanid=1100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-
symmetric=TRUE"
!
```

The card will not crash if either dot1q range or IDLE-Timeout is absent from the downloaded configuration.

Workaround: Configure radius to either not send an idle-timeout value or to not send a dot1q range.

- CSCtr06867

  Symptoms: There is no response to SNMP queries of the MIB objects:

  ```
  1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive
  1.3.6.1.4.1.9.9.276.1.1.2.1.12 cieIfHighSpeedReceive
  ```

  The OID is incorrect in the MIB definition.

  Conditions: This symptom is observed when SNMP walk is not returning any data for the following OIDs:

  ```
  "cieIfSpeedReceive"            "1.3.6.1.4.1.9.9.276.1.1.2.1.11"
  "cieIfHighSpeedReceive"        "1.3.6.1.4.1.9.9.276.1.1.2.1.12"
  ```

  Workaround: There is no workaround.

- CSCtr37182

  Symptoms: XAUI coding errors are seen on the console.

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

  Workaround: There is no workaround.