Caveats in Cisco IOS XE 3.4S Releases

This chapter provides information about caveats in Cisco IOS XE 3.4S releases.

Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the "Caveats for Cisco IOS XE Release 2" section at the following location:

http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

This chapter contains the following sections:

Caveats in Cisco IOS XE 3.4S Releases

Caveats describe unexpected behavior. 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 chapter.

This section describes caveats in Cisco IOS XE 3.4S releases.

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

- Symptom—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/pcgi-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.)

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

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

This section contains the following topic:

Resolved Caveats—Cisco IOS XE Release 3.4.6S

- 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.

- CSCtr88785

  Symptoms: 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.

- CSCts01813

  Symptom: FMAN FP crashes while executing “show platform hardware qfp active feature cef-mpls prefix mpls [label]”

  Conditions: This symptom occurs while executing “show platform hardware qfp active feature cef-mpls prefix mpls [label]”

  Workaround: There is no workaround.

- 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.

- CSCty31407

  Symptom: Netsync configuration for E1 (option 1) is not working.

  Conditions: When you configure R0 as netsync source, the netsync source does not lock (only option 1), but option 2 works fine.

  Workaround: There is no workaround.

- CSCty51453

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

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

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

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

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

- CSCuc42083

  Symptom: fman_fp core file is seen.

  Conditions: This symptom is observed when you configure GreoIPsec with tunnel protection and configure more than 1000 route-maps.

  Workaround: There is no Workaround.

- CSCud44854

  Symptom: Hash table is not cleared for ALG during initialization.

  Conditions: This symptom is observed under the following conditions:

  1. Start sip/h323/... traffic
  2. Established NAT session over 60~70K
  3. Send cli combinations with below actions:

  - clear ip nat trans *
  - shutdown inside / outside traffic interfaces
  - remove nat/alg config
  - reconfig nat/alg and unshut interfaces

Workaround: There is no workaround.

- CSCud49494

  Symptom: ESP crashed with multicast service reflection configuration when receiving UDP fragmented packets.

  Conditions: This symptom is observed when multicast service reflection configured and UDP fragments is received on the VIF interface.

  Workaround: There is no workaround.

- CSCud66955

  Symptoms: 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.

- CSCud92837

  Symptom: The aggregation-type prefix-length of PfR can not be configured less then 16. If so, the number of learned prefix will be much less then it should be.

  Conditions: This symptom is observed when PfR is enabled.

  Workaround: The aggregation-type prefix-length of PfR is better to be configured bigger then 24.

- CSCue32352

  Symptom: Non-hdlc traffic (Non standard but customer defined traffic) coming through HDLC interface gets dropped by Cisco ASR 1000 Series routers.

  Conditions: This symptom occurs in normal L2TPv3 configuration.

  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.

- 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.

- CSCug59930

  Symptom: RP and other FRUs go down and get stuck in disabled state on a 13RU-chassis. This issue is so far seen only on Cisco IOS XE 3.4 throttle branch. Cisco IOS XE 3.5 onwards has not seen this issue.

  Conditions: This issue is caused by stuck midplane-lock acquired but not freed. There is a field notice about defective power supplies on Cisco ASR 1013 chassis. Please use following link and power supply module serial number to check if the power supply modules are affected.

  http://www.cisco.com/en/US/ts/fn/635/fn63555.html

There is a possibility of defective power supplies causing/exposing above issue.

Workaround: There is no workaround.

- CSCug88265

  Symptom: Looking at the output of "show platform software process list r0 sort memory", the memory of "fman_rp" keeps increasing.

  Conditions: This symptom is observed when this box is configured as PfR border router and enabled.

  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.

- CSCuh38488

  Symptom: An ASR with zone-based firewall enabled may drop SIP INVITE packets with the following drop reason:

  ```
  Router#show plat hardware qfp active feature firewall drop
  ------------------------------------------------------------------------------- Drop
  Reason Packets
  ------------------------------------------------------------------------------- L7
  inspection returns drop 1 Router#
  ```

  Conditions: This symptom is observed when the application (L7) inspection for SIP is be enabled for the flow.

  Workaround: Any of the following workarounds are applicable:

  1) Disable the port-to-application mapping for SIP with the **no ip port-map sip port udp 5060** command. This prevents ZBF from treating UDP/5060 as SIP. Instead, it is treated as simple UDP.

  2) Use the "pass" action in both directions instead of "inspect". This disables all inspection (even L4) for the traffic.

Resolved Caveats—Cisco IOS XE Release 3.4.5S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.5S.

- 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.

- 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: This symptom is observed 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.

- CSCts40043

  Symptoms: A Cisco router may crash due to a segmentation fault.

  Conditions: This symptom is observed when a fail-close ACL is applied to the Gdoi crypto map in GETVPN implementation.

  Workaround: There is no workaround.

- CSCts72911

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

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

  Workaround: There is no workaround.

- CSCtt35379

  Symptoms: The Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  Conditions: This symptom can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

  Workaround: Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 September 2012 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

  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 7.1/5.9:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2012-4617 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

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt94440

  Symptoms: The Cisco ASR 1000 series router RP may reload.

  Conditions: This symptom is observed when an etoken is in use and the **show crypto eli all** command is issued.

  Workaround: Avoid using the **show crypto eli all** command. However, you can use the **show crypto eli** command.

- CSCtt99627

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

  Conditions: This symptom 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.

- CSCtu22167

  Symptoms: SP crashes.

  Conditions: This symptom is observed under the following conditions:

  - When unicast prefixes have local labels.
  - When the tunnel is the next-hop for those prefixes.
  - When the topology is modified (that is, when you remove or shut down the physical interface) so that the tunnel's destination address is reachable via the tunnel.

  Workaround: Ensure that the tunnel endpoint peer does not advertise the prefixes to reach the tunnel endpoint.

- 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.

- CSCtu40028

  Symptoms: The SCHED process crashes.

Conditions: This symptom occurs after initiating TFTP copy.

Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtw46061

  Symptoms: The following output shows the leaked SA object continuing to be in the "OBJECT_IN_USE" state. The state is supposed to be changed to OBJECT_FREEING by crypto_engine_delete_ipsec_sa(). This is in turn being called by ident_free_outbound_sa_list().

```
shmcp-fp40#sh crypto eli
Hardware Encryption : ACTIVE
Number of hardware crypto engines = 1

CryptoEngine IOSXE-ESP(14) details: state = Active
Capability    : DES, 3DES, AES, RSA, IPv6, GDOI, FAILCLOSE

IKE-Session   :     0 active, 12287 max, 0 failed
DH            :   211 active, 12287 max, 0 failed
IPSec-Session :   323 active, 32766 max, 0 failed
```

  Conditions: This symptom is observed on a Cisco ASR 1000 series router.

  Workaround: There is no workaround.

- CSCtw46229

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

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

  Workaround: Ensure that all your PPP connections stay stable.

- CSCtw61192

  Symptoms: When the **redistribute static** command has the *route-map* and the *set tag* arguments, and you enter the **no redistribute static** command, the router sends out only one query and the remaining routes get stuck in active state indefinitely.

  Conditions: This symptom is observed only when you set a tag to a redistributed route.

  Workaround: There is no known 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: This 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.

- 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.

- 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” the interface with the QMOVESTUCK error message, remove QoS policies on the interface and subinterfaces, and remove the interface from the T1/T3 controller. Then, rebuild the configuration.

- CSCtw95466

  Symptoms: When a large number of Ethernet or VLAN xconnect sessions are configured on a Cisco 7600 router, the Supervisor Processor may reload.

  Conditions: This symptom is observed when **aaa new-model** is configured.

  Workaround: Configure **no aaa new-model**.

- 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: This symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtw99991

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

  Conditions: This symptom is observed on a Cisco 7600 router with ES+ LC running Cisco IOS interim Release 15.2(01.16)S.

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: This symptom occurs when you configure REP.

  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 multiple routes go down at the same time, and a query arrives from the neighbor router. Finally, the neighbor detects SIA for the affected router and the neighbor state is flap. However, the active entry is remaining after that, and the route is not updated.

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

- CSCtx11740

  Symptoms: The traffic convergence takes longer because of additional/unwanted traffic is punted to CPU as we do not have *,GM code changes. The *,GM entries help drop the traffic that is not needed by MFIB (PI) code.

  Conditions: This symptom is observed with link and node failures in dual-home scenarios.

  Workaround: There is no workaround.

- CSCtx15650

  Symptoms: PFR dynamic route-map Cisco IOS is not downloaded to hardware on the Cisco ASR 1000 or the dynamic route-map is present; however, the route-map sequences are not processed in sequential order.

  Conditions: This symptom is observed with the Cisco ASR 1000 platform.

  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.

- CSCtx35064

  Symptoms: Traffic remains on a blackholed path until the holddown timer expires for a PfR monitored traffic class. Unreachables are seen on the path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  - MC reroutes traffic-class out a particular path (BR/external interface) due to an OOP condition on the primary path.
  - Shortly after enforcement occurs, an impairment on the new primary path occurs, causing blackhole.
  - PfR MC does not declare OOP on the new primary path and attempts to find a new path until the holddown timer expires, which causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx49073

  Symptoms: Free space check fails and IOS core dump never completes.

  Conditions: This symptom is observed when there is not enough storage media space for Cisco IOS core dump.

  Workaround: Make sure there is enough storage space for Cisco IOS core dump.

- CSCtx49098

  Symptoms: A crash occurs at udb_pre_feature_unbind_cleanup.

  Conditions: This symptom is observed when a complex 3 level HQoS policy is configured on the interface and it is manipulated with changes.

  Workaround: Do not manipulate the QoS policy while it is being used or avoid using the same child policy multiple times in the parent policy.

- CSCtx51420

  Symptoms: After reloading the router on Cisco IOS Release 15.2(2)S (or other affected code), the router begins to crash on bootup. The following error may also be seen:

  ```
  %SYS-2-NOBLOCK: printf with blocking disabled. -Process= "TPLUS", ipl= 7, pid=
  459
  ```

  Conditions: This symptom is observed when AAA/TACACS is configured and is operational on the device.

  Workaround: Removal of AAA system accounting will prevent the crash.

- CSCtx57146

  Symptoms: SIP SPAs go in the out of service state in a scaled subinterface configuration (more than 2000 subinterfaces on a single Gigabit Ethernet port).

  Conditions: This symptom occurs while performing ISSU between the iso1-rp2 and iso2-rp2 Cisco IOS XE Release 3.6S throttle image. After ISSU runversion, the SIP SPAs go in the out of service state. This issue is seen in a heavily scaled configuration. This issue is observed when there are 2000 to 3000 subinterfaces on a single SPA and the following limits are exceeded:

  ```
  Overall Dual stack VRFs per box : 2800
  Dual stack limit on interface : 1000
  ```

  Workaround: This issue is not seen in the following scenario:

  1. Before doing a load version from RP0 (initial active), issue the following command:

     ```
     asr1000# show ipv6 route table | inc IPv6
     ```

  2. Note down the number of IPv6 route tables in the system.
  3. Do a load version.
  4. Wait for standby to come up to Standby hot.
  5. Enable the standby console from RP0 (active).

     ```
     asr1000#configure terminal
     Enter configuration commands, one per line.
     End with CNTL/Z.
     asr1000(config)#
     asr1000(config)#redundancy
     asr1000(config-red)#main-cpu
     asr1000(config-r-mc)#standby console enable
     ```

  6. Log in to the standby console and issue the following command:

     ```
     asr1000-stby# show ipv6 route table | inc IPv6
     ```

  Then, note down the number of IPv6 route tables in standby. If the number is less than the number noted at step 2, wait for some time and reverfiy till it reaches the number noted in step 2.

  7. Issue ISSU runversion from RP0 (active).

- CSCtx57784

  Symptoms: Device crashes while configuring “logging persistent url”.

  Conditions: This symptom occurs when the destination file system has zero free bytes left.

  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.

- CSCtx67474

  Symptoms: An update message is sent with an empty NLRI when the message consists of a 2-byte aspath in ASPATH attribute and a 4-byte value aggregate attribute.

  Conditions: This symptom can occur when there is a mix of 2-byte and 4-byte attributes in the update message and the message is sent from a 2-byte peer and there is a 4-byte aggregator attribute.

  Workaround: Move all the 2-byte AS peers to a separate update-group using a nonimpacting outbound policy like “advertisement-interval”.

- CSCtx73691

  Symptoms: The Cisco ASR 903 router forwards packets while in HSRP standby mode.

  Conditions: This symptom occurs when the Cisco ASR 903 is running HSRP and the HSRP session flaps.

  Workaround: There is no workaround.

- CSCtx74051

  Symptoms: When doing an ISSU downgrade, IPv6 flexible netflow monitors may be displayed and the running configuration is shown with incorrect sub-traffic types.

  Conditions: This symptom occurs upon a downgrade to Cisco IOS Release 15.2(1)S (Cisco IOS XE Release 3.5S). The monitors affected are those applied to IPv6. For example, CLI such as:

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

  Workaround: Netflow code should still capture packets as expected on Cisco IOS Release 15.2(1)S. However, a reboot of the device should be done before saving the running configuration as the affected configuration saved will be incorrect and so will then fail to work on startup.

- CSCtx74342

  Symptoms: After an 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: This symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 seconds default).

  Workaround: Configuring the SPF throttle timer can change the interval.

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

  ```
  Router show 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
```

- CSCtx80078

  Symptoms: Packets are getting punted to the CPU or being forwarded with EVC MAC security.

  Conditions: This symptom is seen with implicit deny of packets with routable IPv4 header.

  Workaround: There is no workaround.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: This symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- 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.

- CSCtx85489

  Symptoms: A memory leak is followed by a router crash.

  Conditions: This symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 15.2(2)S. Configuring and unconfiguring PBR “N” number of times from an interface triggers the crash. The root cause for this issue is that each time when PBR is configured and unconfigured, memory is leaked.

  Workaround: There is no workaround.

- CSCtx90705

  Symptoms: Several MPLS features fail for ping.

  Conditions: This symptom is observed during ISSU downgrade.

  Workaround: There is no workaround.

- CSCtx91831

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

  Conditions: When we have an IP address configured for the BD, the following sequence of configurations puts the box in a state where the corresponding IP address is not installed in the routing table.

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

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

  vlan <vlan-id>
  ```

  This issue seen only when we have SVI and BD EFP and will not be seen for SVI and trunk ports.

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

- 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.

- CSCtx94772

  Symptoms: xconnect cannot be configured on an SVI when an RFP having the same BD is configured with pop 2 symmetric.

  Conditions: This symptom is observed only when EFP is configured first and then the xconnect over SVI.

  Workaround: Configure the xconnect over SVI before configuring the RFP with the same pop 2 and same BD.

- 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 linecard.

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

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

- CSCty08070

  Symptoms: The router may print an error message and traceback similar to the following example:

  ```
  %SCHED-STBY-3-THRASHING: Process thrashing on watched
  boolean 'OSPFv3 Router
  boolean'. -Process= "OSPFv3R-10/4/2", ipl= 5, pid= 830router ospf
  -Traceback= 7235C3Cz 7235F1Cz 6A5F7A8z 6A6168Cz 50DA290z 50D3B44zv
  ```

  Conditions: This symptom is observed when the affected OSPFv3 router is configured, but the process does not run because it has no router-id configured. Further, an area command is configured, for example, "area X stub".

  Workaround: Configure "router-id" so that the process can run.

- 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 a routed pseudowire.
  - The core facing card is ES+.
  - The 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 a physical interface only (that is, without a tunnel).
2. TEFRR over the port-channel interface.
3. This issue will not be observed on ES20.
4. This issue will not be observed in Cisco IOS Release 15.0(1)S and later releases.

- CSCty16620

  Symptoms: The backup pseudowire in SVIEoMPLS does not come up after reloading the router.

  Conditions: This symptom is seen under the following conditions:

  1. Remote PE on the backup PW does not support pseudowire status TLV.
  2. The "no status TLV" is not configured in pw-class used in the PW, which does not support pseudowire status TLV.

  Workaround:

  Proactive workaround: Configure "no status TLV" into the pw-class used if the remote side does not support status TLV.

  Reactive workaround: Reprovision the backup pseudowire after reload.

- CSCty17538

  Symptoms: IP and IPv6 traffic may be dropped when "cts role-based sgt-map" is configured.

  Conditions: This symptom is observed with nonhardware and non-CEF-switched traffic egressing an interface when an sgt-map is configured with a more specific prefix than the interface's prefix.

  Workaround: Configure the mask of the sgt-map to match that of the interface's address.

- CSCty23747

  Symptoms: MAC address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  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.

- CSCty28384

  Symptoms: The police actions are not accepted if given in different commands.

  Conditions: This symptom occurs if police actions are given in different commands, and they are not accepted.

  Workaround: Configure the police actions in a single command.

- CSCty28796

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

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

  Conditions: This symptom is observed on Cisco ME3600X and ME3800X.

  Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

  Conditions: This symptom is observed when bringing up PPPoE sessions with a configured invalid local IP address pool under a virtual-template profile and "aaa authorization network default group radius" on the box with no radius present. No IP address is assigned to the PPPoE Client.

  Workaround: There is no workaround.

- CSCty32728

  Symptoms: CPU hog is seen when an MVPN configuration is replaced with another using the **configure replace** command.

  Conditions: This symptom is observed on a stable MVPN network when replacing the configuration with dual-home receiver/source configuration once the router comes up with the tunnel.

  Workaround: There is no workaround.

- CSCty34200

  Symptoms: In an MVPN scale environment, a crash is observed after "no ip multicast-routing". A memory leak is observed after changing the data MDT address.

  Conditions: This symptom is seen in an MVPN scale scenario.

  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 the hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: This 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.

- CSCty42626

  Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.

  Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list) the Cisco c3925E, c3945E, c2951, c3925, c3945, c7200/VAM2+/VSA, possibly VPNSPA on c7600/Catalyst 6000, 819H, and ISR G2 routers with ISM IPSec VPN accelerator.

  Workaround: There is no workaround.

- CSCty45999

  Symptoms: The "aps group acr 1" line disappears after power off 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 and “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.

- CSCty46273

  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) may crash when the connected routes in the RIB flap.

  Conditions: This symptom is observed when LISP tracks the reachability of routing locators (RLOCs) in the RIB. For the crash to occur, a locator being watched by LISP must be covered by a route that is itself covered by a connected route. If both these routes are removed from the RIB in close succession, there is a small possibility that the race-condition resulting in this crash may be hit.

  Workaround: There is no workaround.

- CSCty49656

  Symptoms: A crash is observed when executing the **no ip routing** command.

  Conditions: This symptom is observed under the following conditions:

  1. Configure OSPF.
  2. Enable multicast.
  3. Create several (>6000) routes in the network to be learned by OSPF.
  4. Wait for OSPF to learn all the (>6000) routes from the network.

  Finally, executing the **no ip routing** command may crash the box.

  Workaround: There is no workaround.

- CSCty51088

  Symptoms: On a Cisco ME 3600X or Cisco ME 3800X, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since no (S2,G) entry is formed.

  Conditions: This symptom is observed when the receiver interface is already a source interface for another multicast stream.

  Workaround: There is no workaround.

- CSCty52047

  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).

  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.

  Workaround: Manually delete the stuck isakmp session:

  ```
  clear crypto isakmp conn-id
  ```

  You can get the conn-id from the output of the **show crypto isakmp sa** command.

- CSCty53654

  Symptoms: Traffic through 6RD tunnel is getting dropped. In the **show mls cef ipv6** *prefix* **detail** command, the **vlan** *vlanid* field will be present. On the 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.

- CSCty54319

  Symptoms: OSPF and protocols using 224.0.0.x will not work btw CE-CE over a VLAN.

  Conditions: This symptom occurs when IGMP snooping is disabled.

  Workaround: Toggle IGMP snooping two times.

- 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.

- CSCty58656

  Symptoms: A Cisco 7600 series router with ES+ module may crash.

  Conditions: This symptom is observed with the QoS policy map that has a name hash that is the 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.

- CSCty60467

  Symptoms: SSM ID leak issues or SSM stats show unprovisioned segment counters. The leak can be observed with the command **show ssm stats**. Look for the following in the output:

```
Segment States Counters
  Type           Class          State          Count
  IP-SIP         SSS            Unprov         1050  <<< the count
indicates the IDs are getting leaked.

Alarm: Counter reaches 1 Million: indicates you may be nearing ID exhaust
state.
```

  Conditions: This symptom is observed with the following steps:

  1. Configure “ip dhcp ping packets 10” on an ISG.
  2. Initiate an L2-connected ISG DHCP session by triggering DHCP discover from the client.
  3. Start TCP traffic from the client immediately.
  4. The issue can be observed commonly on high CPS (greater than best practice).
  5. This issue is observed in Cisco IOS XE Release 3.2S and Cisco IOS XE Release 3.5S.

  Workaround: Configuring “ip dhcp ping packets 0” will bring down the rate of SSM ID leak.

- CSCty61212

  Symptoms: The removal of crypto map hangs the router.

  Conditions: This symptom is observed with the removal of GDOI crypto map from the interface.

  Workaround: There is no workaround.

- CSCty67401

  Symptoms: When traffic arriving on the ingress EVC BD interface is priority-tagged, the cos value of traffic egressing out of EVC with single-encap configuration is incorrectly set to 0.

Conditions: This symptom is observed on the Cisco ME3600 2RU, running Cisco IOS Release 15.2(2)S, when the cos value of a packet going out of the EVC BD port with single-encap is incorrectly set to 0.

Workaround: There is no workaround at present.

- 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.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

```
policy-map sub-interface-account
 class prec1
  police cir 4000000 conform-action transmit  exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit  exceed-action drop
  account
 class prec3
  account
  class class-default fragment prec4
  bandwidth remaining ratio 1
  account

policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
  bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
 class class-default
  queue-limit 80 packets
```

  Workaround: There is no workaround.

- CSCty69631

  Symptoms: Multicast RPF failures are observed with GRE tunnels and MSDP in the Cisco ASR 1000 router. This issue may occur when multicast traffic flows over GRE tunnels. This issue does not occur consistently.

Conditions: This symptom occurs when multicast traffic flows through the GRE interface.

Workaround: Reload the Cisco ASR 1000 box.

- CSCty71843

  Symptoms: Tracebacks observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.

  Conditions: This symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This issue is observed when a router is reloaded with the L2VPN configurations.

  Workaround: There is no workaround.

- CSCty73142

  Symptom: An IPC Init failure occurs during downgrade, which makes the standby reload continuously.

  Conditions: This symptom occurs when you perform an ISSU downgrade from Cisco IOS XE Release 3.6S to Cisco IOS XE Release 3.5.1S or Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCty73817

  Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message:

  ```
  %PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD:
  Index addition failed, reloading self
  ```

  Conditions: This symptom occurs when all the following conditions are met:

  1. There is a large amount of sessions.
  2. The QoS Policy Accounting feature is used.
  3. Switchover is done.

  Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command **clear pppoe all**.

- CSCty74129

  Symptoms: The router may cause REP to reconverge during RSP switchover.

  Conditions: This symptom occurs when REP traffic is passing between two Cisco ASR 903 routers and you perform an RSP switchover.

  Workaround: There is no workaround.

- CSCty76106

  Symptoms: A crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes, and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty79381

  Symptoms: MST fails to peer and displays Dispute State, causing traffic loss.

Conditions: This symptom is observed upon SSO.

Workaround: To enable the port, reconfigure MST or flap the ports.

- CSCty81700

  Symptoms: When a remote PE reloads in an MVPN network, it causes a memory leak.

  Conditions: This symptom occurs when core interface flap or remote PE node reloads, causing a small amount of memory leak. If the node stays up experiencing a lot of core interface/remote PE outages, it can run out of memory and fail to establish PIM neighborship with remote PEs.

  Workaround: There is no workaround. As a proactive measure, the user can periodically (depending on n/w outages) run the **show memory debug leak chunk** command and reload the node, if there are a lot of memory leaks reported by this command.

- CSCty82888

  Symptoms: Removing an ATM Permanent Virtual Path (PVP) by the **no atm pvp** command while it is configured with the **xconnect** command causes a memory leak. This can be observed using the **show circuit memory** command:

  ```
  Router#show acircuit memory | include AC ctx chunks
    AC ctx chunks             :        200/32820      (  0%) [      2] Chunk
  ```

  Also, on a dual-RP system with stateful switchover enabled, if the PVP is immediately reconfigured and the **xconnect** command is added, the standby RP may reload.

  Conditions: These symptoms have been observed on Cisco routers that are running Cisco IOS Release 15.2(2)S.

  Workaround: Unconfigure the xconnect using the **no connect** command before removing the PVP.

- CSCty83357

  Symptoms: ACL denied packets are getting punted to host queue, leading to flaps in routing protocols.

  Conditions: This symptom occurs when ACL is configured with src IP match, and packets are being denied by the ACL. The packets are punted to the CPU.

  Workaround: There is no workaround.

- CSCty85634

  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) without an EID-table for the default VRF fails to maintain its LISP map-cache during an RP switchover. After the switchover, the existing remote EID entries in CEF eventually expire and new data packet signals result in repopulation of the LISP map-cache, thus resuming normal operation.

  Conditions: This symptom occurs in a LISP configuration that contains EID-tables for VRFs other than the default and does not contain an EID-table for the default VRF.

  Workaround: Configure an EID-table for the default VRF before the switchover with some LISP configuration such as “ipv4 itr”.

- CSCty91955

  Symptoms: L2-switched traffic loss within a BridgeDomain routed traffic via an SVI experiences no loss.

  Conditions: This symptom occurs with BridgeDomain that has both tagged and untagged EVCs. Issue should not happen with like-to-like scenario.

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

- CSCty93290

  Symptoms: Momentary traffic loss of multicast traffic with QoS configuration on EFP is observed.

  Conditions: This symptom is seen under the following conditions:

  1. Have multiple VLANs in the OIF list.
  2. Each VLAN should have only one EFP/sp.
  3. Have QoS configured on EFPs.

  Workaround: There is no workaround.

- 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

  Symptoms: The 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.

  Conditions: This symptom is observed with the Cisco IOS Software that 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.

  Workaround: 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

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 September 2012 bundled publication.

  Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link:
  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

  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 7.8/6.4:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-4621 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

- CSCty96263

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. This behavior will be caused by loss of pseudowire status packets. Lack of a classification mechanism for these packets prevents user from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty96579

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. This behavior will be caused by loss of vital OAM packets (for example. AIS/LDI, LKR). Lack of a classification mechanism for these packets prevents from protecting them with a QoS policy.

  Workaround: There is no workaround.

- 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 blackholed when TE auto-backup is enabled on the midpoint router and FFR is configured on the P2MP TE tunnel headend.

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

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

- CSCtz03779

  Symptoms: The standby RSP crashes during ISSU.

  Conditions: This symptom occurs when you perform an ISSU downgrade from Cisco IOS XE Release 3.6S to Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCtz04090

  Symptoms: In a VRRP/HSRP setup, traffic from particular hosts is getting dropped. Ping from the host to any device through the VRRP routers fails.

  Conditions: This symptom is usually seen after a VRRP/HSRP switchover. The packet drops because of some packet loop that is created between the routers running VRRP/HSRP.

  Workaround: A clear of the MAC table on the new VRRP master usually restores the setup to working conditions.

- CSCtz13451

  Symptoms: A Cisco ME 3800X and Cisco ME 3600X switch may experience CPU HOG errors and then a watchdog crash or memory corruption.

  Conditions: This symptom is observed when running many of the **show platform mpls handle** commands. The switch may crash.

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

  Workaround: Do not run the commands as they are for development use.

- CSCtz14980

  Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.

  Conditions: This symptom is observed when you have “crypto map GETVPN_MAP gdoi fail-close” configured and image is Cisco IOS XE Release 3.6S or Cisco IOS XE Release 3.7S.

  Workaround: There is no workaround.

- CSCtz16622

  Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.

  Conditions: This symptom is seen with label pop action at the Edge-LSR.

  Workaround: There is no workaround.

- CSCtz23638

  Symptoms: The following error message is seen on the console:

  ```
  PLIM driver informational error txnpTooLittleData
  ```

  Conditions: This symptom is observed when the SIP40 carrier card is present in the router, along with any of the below SPAs:

  SPA-1CHOC3-CE-ATM

  SPA-1XCHOC12/DS0

SPA-1XCHSTM1/OC3

SPA-1XCHSTM1/OC3W(Same SPA as SPA-1XCHSTM1/OC3. Included in “SB” bundles)

special pricing)

SPA-24CHT1-CE-ATM *

SPA-2CHT3-CE-ATM

SPA-2X1GE-SYNCE

SPA-2XCT3/DS0

SPA-2XT3/E3

SPA-4XCT3/DS0

SPA-4XCT3/DS0-WE(Same SPA as SPA-4XCT3/DS0. Included in “SB” bundles - special pricing)

SPA-4XT3/E3

SPA-8XCHT1/E1

SPA-DSP

SPA-WMA-K9

Workaround: There is no workaround.

- CSCtz27782

  Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.

  Conditions: This symptom occurs when interface is in OAM RLB slave mode.

  Workaround: There is no workaround.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, the 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 the access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz32521

  Symptoms: In interop scenarios between the Cisco CPT and Cisco ASR 9000 platforms, in order to support the transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Conditions: This symptom occurs in interop scenarios between Cisco CPT and the Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require the Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Workaround: There is no workaround.

- CSCtz35467

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

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

  Workaround: To be preventive, use “police cir <absolute>” instead of “police cir percent x”. To be reactive, use EEM applet/script.

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

- CSCtz38119

  Symptom: The router does not complete a MAC address flush on the receiving side of a VPLS pseudowire.

  Conditions: This symptom occurs when the router receives a Layer 2 MAC withdrawal over a VPLS pseudowire.

  Workaround: There is no workaround.

- CSCtz40435

  Symptoms: The L4 port-range security ACL does not work on EVC.

  Conditions: This symptom is observed when security the ACL containing L4 port range operation that is applied on EVC. The behavior is not as expected. The same works on the physical interface.

  Workaround: Add support for the L4 port range operation similar to the case of applying it on the physical interface.

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

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

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCtz44963

  Symptoms: CCDB is not populated after removing/readding EFP.

  Conditions: This symptom occurs when CCDB is not populated after removing/readding EFP.

  Workaround: Reload the router.

- CSCtz45057

  Symptoms: High CPU is seen on a Cisco ME 3800X switch.

  Conditions: This symptom occurs when loop of OTNIFMIB causes CPU Hog/Crash on a Cisco ME 3800X switch during pulling from PPM.

  Workaround: Disable OTNIFMIB while pulling from PPM, which is not supported or required on the Cisco ME 3800X and ME 3600X switches.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using the range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is observed with IPv4 and IPv6 with L4 port range operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME3800 switches.

  Workaround: There is no workaround.

- CSCtz54823

  Symptoms: The configuration is getting locked on the chopper SPA.

  Conditions: This symptom occurs 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 startup and reload the system to get back to configuration mode.

- CSCtz74189

  Symptoms: Occasionally, the system hangs at bootup with the following signature in the bootlogs. The system will not respond to break character keys.

```
 Configuring Freq Synthesizer 2^M
 Synthesizer PLL  2 locked successfully^M
 Configuring Freq Synthesizer 3^M
 Synthesizer PLL  3 locked successfully^M
 Configuring Freq Synthesizer 4^M
 Synthesizer PLL  4 locked successfully^M
 TDM Processor has been configured in iter(1)^M <<<<<<<<<<<< HANG
```

  Conditions: This symptom occurs in normal reload conditions, or on a next reload of the software after a system power cycle.

  Workaround: Requires a system power cycle.

- CSCtz75228

  Symptoms: On a power cycle or a reload condition, the system may stall occasionally after the following console logs are printed.

```
<snip
Finished memctrl.h, apply WinHMS Errata...
Initialize Winpath
Initializing interrupt controller
Initialization of Winpath Complete
loading program at addr: 0xE2C00000, size: 0x0007A648
Enable the MIPS Core0
Before minimon_init() call... <<<<<<<<<<<HANG
-----  minimon 1st 64 bytes ------
C00BD108:
```

  Conditions: This symptom may occur during a system reload.

  Workaround: A power cycle is required, and the subsequent reload may not be impacted.

- CSCtz75380

  Symptoms: A Cisco ASR 1000 series router sends malformed radius packets during retransmission or failover to a secondary radius server, for example, Cisco CAR.

  ISG log if secondary radius server is installed in the network:

  %RADIUS-4-RADIUS_DEAD: RADIUS server <ip-secondary-Radius-Server>:1645,1646 is

  not responding.

  %RADIUS-4-RADIUS_ALIVE: RADIUS server <ip-secondary-Radius-Server>:1645,1646 is

  being marked alive.

```
Radius-Server Log:
13:23:01.011: P78: Packet received from 10.0.0.1
13:23:01.011: P78: Packet successfully added
13:23:01.011: P78: Parse Failed: Invalid length field - 63739 is greater than 288
13:23:01.011: Log: Packet from 10.0.0.1: parse failed <unknown user>
13:23:01.011: P78: Rejecting Request: packet failed to parse
13:23:01.011: P78: Trace of Access-Reject packet
13:23:01.011: P78:    identifier = 40
13:23:01.011: P78:    length = 21
13:23:01.011: P78:    reqauth = 23:<snip....>
13:23:01.011: P78: Sending response to 10.0.0.1
```

```
13:23:01.011: Log: Request from 10.0.0.1: User <unknown user> rejected
(MalformedRequest).
13:23:01.011: P78: Packet successfully removed
```

Conditions: The issue can occur during retransmission of radius access requests or if radius packets are sent to a secondary radius server.

Workaround: There is no workaround.

- CSCtz80571

  Symptoms: Rewriting the ingress tag configuration is not accepted.

  Conditions: This symptom occurs when you create a port-channel1 interface and then create a port-channel2 interface.

  Workaround: There is no workaround.

- CSCtz83311

  Symptoms: In the bootlog, the following strings may be observed:

  ```
  "MCB timeout"
  ```

  Occasionally, these messages also are followed by a Gigabit Ethernet port link down for any of the ports Gig 0/1-Gig 0/8. A **shut/no shut** may not recover the link down condition.

  Conditions: This symptom occurs during a system reload. It may also occur if a **media-type** command is issued to the first eight Gigabit Ethernet ports.

  Workaround: Do not configure “media-type rj45” for the first eight ports either at bootup time or configurations if you are using an image that does not have this fix.

- CSCtz85225

  Symptoms: The RF functionality does not work on 10GE interfaces.

  Conditions: This symptom is observed on the Cisco ASR 903 router.

  Workaround: There is no workaround.

- CSCtz88289

  Symptoms: It is observed that in a Cisco ME 3600-24CX unit, which is subjected to 100 consecutive image reloads, there is a system bootup hang in this area. The system stalls indefinitely and does not respond to console keystrokes like break keys.

  ```
  <bootup snip>

   I2C Bus Initialization begins
   Margining CPU and Nile board Voltages
   Control FPGA Initialization begins  <<<<System  Hang here
  ```

  Conditions: This symptom may occur during a system bootup.

  Workaround: A powercycle is required, and the next reload may not hit the above condition.

- CSCtz94188

  Symptoms: With AdvancedMetroIPAccess evaluation license and with TDM permanent license xconnect under CEM, ckts are not shown and are not configurable.

  Conditions: This symptom occurs under regular configuration steps.

  Workaround: There is no workaround.

- CSCtz96342

  Symptoms: Inconsistency in a scaled feature license name between Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* and Cisco IOS Release 15.2(2)S:

  ```
  Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* - ScaledServices
  Cisco IOS Release 15.2(2)S      - ScaledMetroAggrServices
  ```

  Conditions: This symptom occurs with an upgrade from Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* to Cisco IOS Release 15.2(2)S, which could impact the scalability feature in below ways:

  - If user already had permanent license before upgrade, it will now downgrade to Eval license.
  - New license for installing ScaledMetroAggrServices cannot be generated as the license tool does not support this feature name.

  Workaround: Upgrade to Cisco IOS Release 15.2(2)S1.

Resolved Caveats—Cisco IOS XE Release 3.4.4S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.4S.

- 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: This symptom is observed with the following conditions:

  - “proxy-arp” is enabled on the client-facing Layer 3 interface.
  - The end device sends a “duplicate address detection” ARP request on its local subnet.

  Workaround 1: Configure **no ip proxy arp** on the 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: A crash is seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: This 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 the “nhrp_cache_info_disseminate_internal” function.

- CSCtq99664

  Symptoms: Traffic does not egress from the interface.

  Conditions: This symptom is observed when the VRF set on the interface is originally configured for the 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.

- 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 the 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, the restarting router (PE, in this case) does not advertise RT constrain filters to the nonrestarting peer (RR, in this case).

  Conditions: This symptom is observed after an SSO in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the nonrestarting 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: This 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: This symptom is observed on an IP PIM multicast network.

  Workaround: There is no workaround.

- CSCtt99627

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

  Conditions: This symptom is observed with 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 symptom 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: This 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 a crash.

  Conditions: This symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: A small buffer leak is seen. The PPP LCP configuration requests are not freed.

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

  Workaround: Ensure that all your PPP connections stay stable.

- CSCtw61872

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

  Conditions: This 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.

- CSCtw64073

  Symptoms: Traceback is seen with the "%CPPOSLIB-3-ERROR_NOTIFY" error message.

  Conditions: This symptom is observed when the Cisco ASR router is processing ACL merge for a given feature set.

  Workaround: FP will crash and restart in most cases; however, in some cases a reboot may be needed.

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience the 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 the interface in the QMOVESTUCK error message, remove QoS policies on interface and subinterfaces, remove theinterface from T1/T3 controller, and then rebuild the configuration.

- 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 subinterfaces can be created.

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

- 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 the neighbor router. Finally, the neighbor detects SIA for the affected router and the neighbor state is flap. However, active entry is remaining after that, and the 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.

- CSCtx32599

  Symptoms: Traceback messages are printed on the console. The device does not experience adverse effects.

  Conditions: This symptom occurs on the console.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCtx74342

  Symptoms: After the 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: This 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
```

- CSCtx81689

  Symptoms: In case of IPv6MVPN, PIM neighbor cannot be established.

  Conditions: This symptom is is only triggered on FP40 or above systems.

  Workaround: Disable MLRE with the **platform multicast lre off** configuration command.

- CSCtx84948

  Symptoms: A Cisco ASR 1000 series router malfunctions after consecutive ESP crashes triggered by CSCtr56576. This symptom is observed when the interfaces are up/up but are not sending traffic. You can also identify this state using the following command:

```
Router#show platform software interface fp active name GigabitEthernet5/0/0
Name: GigabitEthernet5/0/0, ID: 23, QFP ID: 22, Schedules: 4096
Type: PORT, State: disabled, SNMP ID: 16, MTU: 1500   <<<<<<
```

  The output of the command indicates that at the ESP level, the interface is disabled and cannot forward traffic.

  Conditions: This symptom is observed when the Cisco ASR 1000 series router has redundant ESPs and consecutive ESP crashes. This symptom has been caused only by CSCtr56576.

  Workaround: **Shut/no shut** the disabled interface to resume the traffic.

- CSCtx89260

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

  Conditions: This symptom is observed when readding the deleted port-channel interface.

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

- 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: This symptom is observed with a multilink interface flap.

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

- CSCty10285

  Symptoms: WCCP redirection does not happen with a Cisco ASR 1000 router running Cisco IOS XE Release 3.5 RP1.

  Conditions: This symptom occurs when GetVPN is used.

  Workaround: There is no workaround.

- CSCty19713

  Symptoms: The ESP or CPP of a Cisco ASR 1000 series router crashes.

  Conditions: This symptom is observed in the NAT Application Layer Gateway (ALG) for DNS packets.

  Workaround: There is no workaround.

- 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.

- 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: This symptom is observed when the interface is configured with a VRF.

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

- 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.

- CSCty63356

  Symptoms: Memory leak is seen in the cpp_sp_svr process on ESP.

  Conditions: This symptom is observed under the following conditions:

  - A topology of dVTI IPsec as below:

  ```
  dVTI Server (ASR1k) ---- dVTI Client [CES] (7200)
  ```

  - Scale 1000 IKE * 1 VRF * 4 IPsec, total 4K IPsec sessions.

  - Multi-SA enable.
  - CAC=50,DPD=60/15/periodic.
  - Reload CES (7200 platform) every ~20 minutes.
  - ~60M bidirectional traffic.

  Workaround: There is no workaround.

- 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

  Symptoms: Several Cisco 3750X switches in a stack crash. The crashinfo shows vector 0x200 and stack corruption:

```
 C3750E Software (C3750E-UNIVERSALK9-M), Version 15.0(1)SE2, RELEASE SOFTWARE
(fc3)
 Technical Support: http://www.cisco.com/techsupport
 Compiled Thu 22-Dec-11 00:05 by prod_rel_team
 Signal = 10, Vector = 0x200, Uptime = E
 .
 .
 ========= Stack Dump =========================
 Stack Frame Pointer in Context is 0x46DCB0C, at process level
 : INVALID STACK ADDRESS
```

Conditions: The symptom is observed when the switch receives a DHCP using a TLV with a length of 256 or longer. This is not platform-specific.

Workaround: As a workaround, an administrator can disable the DHCP device classifier using the **device-sensor filter-spec dhcp exclude all** command, as shown in the following example:

```
hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
hostname(config)# device-sensor filter-spec dhcp exclude all
hostname(config)# end
```

- 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: This symptom is an extreme corner case/timing issue. This issue has been observed only once on the release image.

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

- 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, Cisco IOS software is not sending refreshed updates to the peer.

  Conditions: This 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 Cisco IOS software 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.

- CSCtz25953

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

  Conditions: This 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.

- CSCtz38558

  Symptoms: The following traceback may be seen on a Cisco ASR 1000 router when processing some IPv6 packets.

```
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579214858 %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM Load at
800268cd HAL start 3fc0 HAL end 413f INFRA start 409e INFRA 4140 NET 340d0
-Traceback=1#002b3a75f6cabf53c25612ed4553871e 804b0d63 804b1204 8046c212 80020708
800268cd 80026cd0 80435955 806509bb
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579433103 %INFRA-3-INVALID_GPM_ACCESS_INFO: 80026cd0 0002fdb0 0002fdd4
0002fdd0 00000002 00000001 00000001 0003413f 00000001 00000000 00000000 00001000
93b9bac0 8ba80000 fffffffd 00201000
```

```
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579587035 %INFRA-3-INVALID_GPM_ACCESS_DATA: e188f4a8aa3ef3a0
205e84e72c9f6761 4486ffd3c38d7e12 b0c71bf4a146b4ba 8e786f7e673d2e56 9308160a565df75c
952e4a0fe2ef327c 1cff673d2be0f8bf 48248a1e150a1ce9 e1386aed768ad28c e6d23cd54b68619e
c49866ce95863bf6 c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a
c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a 8553c53af0e4f16e
```

Conditions: This symptom is observed when the IPv6 packet is malformed.

Workaround: There is no workaround.

Additional Information: The packet will be dropped.

- CSCtz61014

  Symptoms: The system crashes.

  Conditions: This symptom occurs when adding or deleting NTP leap second in NTP master mode.

  Workaround: Do not configure the system as NTP master.

- CSCtz67785

  Symptoms: The Cisco ASR 1000 router may experience a CPP crash.

  Conditions: This symptom occurs when the router is configured for Session Border Controller (SBC). During periods of high traffic, FP reports a lot of media up events to RP, which can crash FP.

  Workaround: If “ip nbar protocol-discovery” is enabled, it may exacerbate the crashes. Removing it may help provide some stability.

- CSCtz69986

  Symptoms: The Cisco ASR 1000 router’s ESP free memory slowly decreases over time (~ 7MB per day).

  Conditions: This symptom occurs when WCCP is configured on interfaces.

  Workaround: There is no workaround, unless the WCCP interface configuration is removed.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 router 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: This symptom is observed when the Cisco ASR router is 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 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.

- CSCtz82711

  Symptoms: Datapath session would

  Conditions: This symptom is observed when SGSN sends echo req before PDP_CREATE_REQ.

  Workaround: There is no workaround.

- CSCtz85102

  Symptoms: Packets with the L2 multicast address and L3 unicast address combination could not be forwarded by L2TPv3 tunnel on the Cisco ASR 1000 router.

  Conditions: This symptom is observed with packets with the L2 multicast address and L3 unicast address combination. This issue is seen with all Cisco ASR 1000 series routers.

  Workaround: There is no workaround.

- CSCtz88716

  Symptoms: The Xe34_dvti_qos feature is errored out when dividing by zero while executing "expr { $actual_rate_data*1.0*$".

  Conditions: This symptom occurs after active and standby RP ISSU upgrade.

  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
  ```

- CSCua27842

  Symptoms: The Cisco ASR 1000 router crashes in Firewall code due to NULL l4_info pointer. Day 1 issue.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:

  1. MPLS L3VPN (PE).
  2. Zone-Based FW/NAT.

3. MPLS and MP-BGP loadbalance is configured towards the upstream router

Workaround: There is no workaround.

- CSCua72048

  Symptoms: When configuring “ipv6 vfr max-fragmentation in/out” at no-default value, the ESP reloads with traceback.

  Conditions: This symptom is observed when “ipv6 vfr max-fragmentation in/out” is configured at no-default value.

  Workaround: There is no workaround.

- CSCua87877

  Symptoms: A crash occurs in ucode.

  Conditions: This symptom is observed with 160cps SIP calls.

  Workaround: There is no workaround.

- CSCua92557

  Symptoms: The active FTP data channel sourced from the outside may not work as expected. Other protocol inspections that expect pinhole or door for connections initiated from the outside may be affected as well.

  Conditions: This symptom was first identified on the Cisco ASR router running Cisco IOS Release 15.1(3)S3 with VASI+VRF+PAT+FW. This issue is seen when the FTP client is on the inside and the active FTP server is on the outside.

  Workaround: Static NAT will work.

Open Caveats—Cisco IOS XE Release 3.4.3S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.3S.

- CSCtr65436

  Symptoms: A Cisco ASR 1000 series router with around 500 spokes starts malfunctioning after it is subjected to MOMBA procedures. This symptom is also observed on a Cisco c3945e Integrated Services router with around 100 spokes.

  Conditions: This symptom is observed in a dual-hub DMVPN and while switching over between hubs.

  Workaround: Do not switch over between hubs.

- CSCts04802

  Symptoms: During vrf transfer, old services are removed but the new service is not applied.

  Conditions: This symptom is observed during a VRF transfer from v1 to v2.

  Workaround: There is no workaround.

- CSCts75470

  Symptoms: Packets do not get intercepted at MD due to multiple ACEs.

  Conditions: This symptom is observed after performing “microcode reload pxf” on IAP and CE1.

  Workaround: Delete the Tap and recreate it.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtu01601

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

  Conditions: The conditions that trigger this symptom are not known.

  Workaround: There is no workaround.

- CSCtu35116

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

  Conditions: This 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.

- 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: There is no workaround.

- CSCtw98200

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

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

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

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

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

- CSCtx11598

  Symptoms: The Router reload causes a Cisco Shared Port Adapter (SPA) failure with the error message “% CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure”.

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

  - none
  - standby reset
  - down

  And further, this failure leads to unexpected system reload.

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

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

- CSCtx15799

  Symptoms: An MTP on a Cisco ASR router sends an “ORC ACK” message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.

  Conditions: This symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.4.3S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.3S.

- 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: This 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 do not accept IPv6 addresses in the VRF interface, but accepts IPv4 addresses:

  - Telnet session accepts both v6 and v4 addresses in the VRF interface.
  - The “Destination unreachable; gateway or host down” message shows in the SSH session to IPv6 addresses in theVRF interface.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

  Conditions: This symptom 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: The router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: This 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/subinterface to this outer (tree state) VLAN.

- CSCtj95685

  Symptoms: A router configured as a voice gateway may crash while processing calls.

  Conditions: This 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 router’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: The router crashes after deleting multiple VRFs. This happens very rarely.

  Conditions: This 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: This 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.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP nonclients 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: This 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: An error message is seen while detaching and reattaching a service policy on an EVC interface.

  Conditions: This 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 fails with the error "% Error in authentication".

  Conditions: This 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: These 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.

- CSCts13474

  Symptoms: ISSU loadversion fails with the message "Unable to read configuration register".

  Conditions: This symptom is observed during superpackage ISSU downgrade from Cisco IOS XE Release 3.5 to Cisco IOS XE Release 3.4.

  Workaround: Execute **issu loadversion** again.

- 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: This symptom is observed during a downgrade scenario where the active is running Cisco IOS Release 15.1 and the standby is running Cisco IOS Release 12.2. Cisco IOS Release 15.1 will be syncing the **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.

- CSCts65564

  Symptoms: In a large-scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This symptom 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: This 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 readd 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: This symptom is observed 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: This symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt37516

  Symptoms: Line card crash with priority traffic when QoS policy is applied.

  Conditions: This symptom is observed with the QoS priority feature.

  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.

- CSCtt53985

  Symptoms: All traffic stops forwarding on a Cisco ASR 1000 series router due to the ESP crashing. Or, half entries with the IP address 239.67.33.205 may show up in the database, which may cause some end stations to be improperly translated. Or, with dynamic configurations two sessions could have the same inside global, but different inside locals (happens very rarely). The workaround for this last condition is to clear the offending session.

  Conditions: This symptom is observed in a rare condition that can result in an ESP crash or bad half entry translations as described above.

  Workaround: For the crash, prevent SNMP from pulling NAT OIDs. This only works sometimes. An upgrade is the best recommended action. This can be done by creating a view. For example:

  ```
  snmp-server view test internet included snmp-server view test 1.3.6.1.4.1.9.10.77.1
  excluded snmp-server community pub view test RO
  ```

  To recover from the bad entries, a reload is required.

- 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.

- CSCtu13951

  Symptoms: Pending objects appear on the active and standby ESP.

  Conditions: This symptom occurs when the edge device to the core link is flapped multiple times for close to two days.

  Workaround: There is no workaround.

- CSCtu20929

  Symptoms: Primary path is disabled when FRR is triggered by a SPA OIR.

  Conditions: This symptom occurs due to a functionality issue and is seen when the primary path and backup path are in different SPAs. The impact is that OSPF is stuck in an INIT state and traffic flow is affected.

  Workaround: Reload the SPA.

- CSCtu24460

  Symptoms: A Cisco ASR 1000 router crashes.

Conditions: This symptom is observed on a Cisco ASR 1000 router that is configured as LNS with per subscriber firewall. Releases affected by this defect: Cisco IOS Release 15.1(3)S, 15.1(3)S1, 15.1(3)S2, and 15.2(1)S.

Workaround: There is no workaround to this issue. Configuring firewall TCP and UDP timers lower than 1200 seconds may reduce the probability of the crash.

- 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 symptom is seen when running large **show** commands like **show tech-support** on the line card via the RP console.

  Workaround: Do not run the show commands frequently.

- 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: This 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: This symptom is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu98960

  Symptoms: The router crashes with scaling of 3500 spokes.

  Conditions: This symptom is observed when scaling to 3500 spokes.

  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: This symptom is observed when the 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".

- CSCtw56012

  Symptoms: On a Cisco ASR 1000 series Asynchronous Object Manager (AOM), pending-ack objects may be seen after removing an ATM multipoint subinterface configured on a SPA-2CHT3-CE-ATM (T3 or E3 mode). This prevents subsequent configuration updates on the same subinterface, resulting in a traffic drop on the PVCs configured under that subinterface.

  Conditions: This symptom occurs when a multipoint ATM subinterface is deleted on a SPA-2CHT3-CE-ATM (T3 or E3 mode).

  Workaround: Use a different subinterface if a reconfiguration of the same PVP and/or PVC is required. For example, the original configuration is:

```
!
interface ATM0/0/1.2000 multipoint
 ip address 10.3.2.1 255.255.255.0
 atm pvp 200
 no atm enable-ilmi-trap
 pvc 200/100
  protocol ip 10.3.2.2 broadcast
  protocol ip 10.3.2.3 broadcast
  encapsulation aal5snap
 !
end
```

  and subinterface ATM0/0/1.2000 was deleted resulting in a pending-ack on the subinterface. Then, to reconfigure the same PVP or PVC, use a different number (ATM0/0/1.2001) for the subinterface:

```
!
interface ATM0/0/1.2001 multipoint
 ip address 10.3.2.1 255.255.255.0
 atm pvp 200
 no atm enable-ilmi-trap
 pvc 200/100
```

```
  protocol ip 10.3.2.2 broadcast
  protocol ip 10.3.2.3 broadcast
  encapsulation aal5snap
 !
end
```

Further Problem Description: When this problem occurs, the AOM pending-ack objects correspond to the deleted multipoint subinterface as shown in the example below:

```
Router#show platform software object-manager fp active statistics
Forwarding Manager Asynchronous Object Manager Statistics

Object update: Pending-issue: 0, Pending-acknowledgement: 1
Batch begin: Pending-issue: 0, Pending-acknowledgement: 0
Batch end: Pending-issue: 0, Pending-acknowledgement: 0
Command: Pending-acknowledgement: 0
Command: Stale-objects: 0

Router#show platform software object-manager fp active pending-ack-update
Update identifier: 269
 Object identifier: 358
 Description: intf ATM0/0/1.2000, handle 44, hw handle 46,
              dirty 0x0, AOM dirty 0x0
 Number of retries: 0
 Number of batch begin retries: 0

Router#show platform software object-manager fp active object 358
Object identifier: 358
 Description: intf ATM0/0/1.2000, handle 44, hw handle 46,
              dirty 0x0, AOM dirty 0x0
 Status: Pending-acknowledgement, Epoch: 0, Client data: 0x1171aac0


Issued action
 Update identifier: 269, Batch identifier: 0
 Batch type: unknown
 Action: Delete
```

Note that this problem is not seen when a point-to-point ATM subinterface is deleted on a SPA-2CHT3-CE-ATM (T3 or E3 mode). It is also not seen on point- to-point, or multipoint ATM subinterfaces on SPA-1XOC3-ATM-V2, SPA-3XOC3-ATM- V2, and SPA-1XOC12-ATM-V2 SPAs.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: This 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: This 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.

- CSCtw69820

  Symptoms: A router with Zone Based Firewall (ZBFW) enabled allows dest.port 0 packets by default. If such packets arrive at a high rate, performance issues may be seen to the extent that OSPF/BGP/EIGRP sessions are dropped, along with high latency on data traffic.

  Conditions: This symptom is observed if ZBFW is enabled and there is TCP/UDP traffic with dest.port 0.

  Workaround: Deny dest.port 0 packets in the ZBFW policy.

- CSCtw71564

  Symptoms: Not all data packets are accounted for in the **show stats** command output of the video operation.

  Conditions: This 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.

- CSCtw76044

  Symptoms: IGMP/MLD information is needed to make IGMP/MLP snooping work.

  Conditions: This 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: A 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: This 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 the 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: This 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: This symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtx01370

  Symptoms: Multicast convergence can be seen in NATted environment for a dual homed Cisco ASR 1000 router CPE running 3.4.1 code (primary and secondary CPE) connecting to different PEs, although multicast traffic is not NATted. The convergence reported in the issue is approximately two minutes.

Conditions: This symptom is observed on a Cisco ASR 1000 router CPE running 3.4.1 code (primary and secondary CPE) connecting to different PEs.

Workaround: The workaround is to prevent RPT to SPT switchover by configuring “ip pim spt-threshold infinity”.

Further Problem Description: The issue is caused by out of order PIM messages send during convergence resulting in outgoing interface on secondary CPE as null.

- 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 symptom 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.

- CSCtx21547

  Symptoms: Ucode and fman-fp crash.

  Conditions: This symptom is observed with a firewall configuration/unconfiguration with HSL configuration in “global inspect parameter-map” after unconfiguring the firewall.

  Workaround: Remove the HSL configuration in “global inspect parameter-map” before unconfiguring the firewall, that is, remove the following configuration: “log flow-export v9 udp destination <IP> <Port>” from “parameter-map type inspect global” or from “parameter-map type inspect- global”.

- CSCtx28483

  Symptoms: A router set up for Cisco Unified Border Element-Enterprise (CUBE- Ent) box-to-box redundancy reloads when certain configuration commands are deconfigured out of the recommended sequence.

  Conditions: This 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 exist.
  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 the default route is updated.

  Workaround: There are two possible workarounds:

  1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.

2. If workaround #1 is not possible, then ensure 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 at fib_fib_src_interface_sb_init.

  Conditions: This symptom is observed with fib_fib_src_interface_sb_init.

  Workaround: There is no workaround.

- CSCtx31175

  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.

  Conditions: This 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 the Cisco ASR 1001 router.
  3. The Cisco ASR 1001 router sends double "Framed-IP-Address" in service-stop accounting for one user's session.

  Workaround: Do not use the **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.

- CSCtx35463

  Symptoms: Output is truncated.

  Conditions: This symptom is observed when displaying **show platform hardware qfp act feature nat data ha**.

  Workaround: There is no workaround.

- CSCtx35498

  Symptoms: ASRNAT B2B: sessions are not aged on the active.

  Conditions: This symptom occurs when the standby stays down.

  Workaround: Do not have the standby down for extended time periods.

- 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: This 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.

- CSCtx37240

  Symptoms: AOM pending-ack objects are seen on Tx Channels of Serial interfaces after router reload.

  Conditions: This symptom is observed with scale setup with hundreds of (channelized) serial interfaces present in the configuration. Reload the router with this configuration.

  Workaround: There is no workaround.

- 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: This symptom is observed with the following 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.

- CSCtx51935

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: This 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

  show mpls traffic-eng link-management summary
  ```

  Workaround: There is no workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through “ip multicast boundary”.

  Conditions: This 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: An 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 symptom can occur 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”.

- CSCtx70505

  Symptoms: Standby FP crashes and gets stuck in INIT standby state after an FP restart.

  Conditions: This symptom is observed with BBA client login and logout with high TPS. Run **sh platform software peer chassis-manager fp standby** periodically.

  Workaround: Reload the router.

- CSCtx71618

  Symptoms: The router crashes at process L2TP mgmt daemon.

  Conditions: This 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 the Cisco ASR1001 router. The IP options field includes the “loose source routing” option.
  2. The Cisco ASR 1001 router receives the packet. The Cisco ASR 1001 router has “no ip source-route” setting in its configuration.
  3. The Cisco ASR 1001 router incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.

  Conditions: This symptom is observed with the Cisco ASR 1001 (2.5G ESP).

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 router may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: This 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: This symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx86069

  Symptoms: The dynamic NAT has a wrong translation that causes multiple inside local addresses to be translated to the same inside global address.

  Conditions: This symptom is observed with the following conditions:

- Cisco IOS XE Release 3.4.2.
- Call flow: multiple sip caller -- proxy --(inside)-- ALG --(outside)-- sip callee.
- Inside dynamic NAT is configured, with one hour timeout.

Steps of reproducing:

1. Make some of the SIPP calls for several hours.
2. After some hours, make calls from idle SIPP.

For the new inside local IP address, NAT will be translated to an existing inside global in the table (without create a new binding in NAT table), which is bound with another inside local address.

Workaround: There is no workaround.

- CSCtx96285

  Symptoms: A configuration of stateful inter-chassis redundancy for NAT may result in packets routing through the standby router and not being processed by the NAT rules, or dropped (NAT is being bypassed).

  Conditions: This symptom is observed after a failover of primary to secondary with all routing protocols forcing traffic to the standby router.

  Workaround: There is no workaround.

- 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: This 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 next-hop 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 next-hop. So if you have a default route received from some neighbors, then that default route will also be flapped.

  Conditions: This symptom 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.

- CSCty17747

  Symptoms: On a Cisco ASR 1000 router that contains an ESP40 forwarding card or on a Cisco ASR 1001 router, there is an issue that prevents Traditional Netflow (TNF) exporters configured under the aggregation cache command from being properly created when the router is reloaded and booted from the startup configuration. A typical command snippet would look like:

```
ip flow-aggregation
 cache prefix
 cache entries 512000
 cache timeout active 5
 export version 9
 export template refresh-rate 5
 export destination 192.168.1.2 9995
 export destination 192.168.3.4 9995
 mask source minimum 32
 mask destination minimum 32
 enabled
!
```

If this configuration is in the startup-configuration and the router is reloaded, the exporter commands will not take effect after the reload and no packets will be exported.

Conditions: This defect has only been observed on either ESP40 forwarding cards or on a Cisco ASR 1001 router. This defect does not occur during manual configuration but only when the router is reloaded and the startup- configuration (or other bootup configuration) is parsed.

Workaround: Reapply the missing exporter configuration manually after the router is already up.

- 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: This 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: The router crashes while doing an SSO without any configurations.

  Conditions: This symptom is observed while doing an SSO.

  Workaround: There is no workaround.

- CSCty46022

  Symptoms: A Cisco ASR 1000 router experiences high ESP CPU constantly.

  Conditions: This symptom is observed when ISG sessions with DHCP initiator are experiencing fragmented traffic and the fragmented traffic has a small packet size. The packets will be punted to ESP CPU and cause it to be busy.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.4.2S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.2S.

- CSCtw45055

  Symptom: 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:

```
Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time
expired) x bytes
Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification
received
Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology
base removed from session Neighbor deleted
```

```
Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology
base removed from session Neighbor deleted
Nov 10 08:10:51.816: %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 neighborship removals, either because of flapping or potentially by manual removal.

Workaround: There is no workaround.

- CSCtu20223

  Symptoms: An unexplained change is observed in the MTU value written in the running configuration.

  Conditions: This symptom is observed with a Cisco ASR 1002 router running Cisco IOS Release 15.1(2)S1.

  Workaround: There is no workaround.

- CSCtw69820

  Symptoms: A router with Zone Based Firewall (ZBFW) enabled allows dest.port 0 packets by default. If such packets arrive at a high rate, performance issues may be seen to the extent that OSPF/BGP/EIGRP sessions are dropped, along with high latency on data traffic.

  Conditions: This symptom is observed if ZBFW is enabled and there is TCP/UDP traffic with dest.port 0.

  Workaround: Deny dest.port 0 packets in the ZBFW policy.

- 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 SXI4, Cisco IOS Release SXI7, Cisco IOS SR Release, Cisco IOS SX Release, and Cisco IOS S Release .

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtu31099

  Symptoms: A crash related to VRRP occurs.

  Conditions: This symptom is observed with VRRP. This issue may be also accompanied with the following error message. Also, if repeated Duplicate address messages are seen, it is because of a misconfiguration.

  ```
  %IP-4-DUPADDR: Duplicate address X.X.X.X on [Interface], sourced by [MAC-Address]
  ```

  Workaround: Use HSRP. If you are currently using owner mode for your configuration, all you need to do is assign a single unique address to the "owner mode" interface so that it does not match the virtual address. Then, assign a high priority to HSRP on this interface, and you will have an equally functionality to before. The only valid reason for not using HSRP would be if you need to operate with another vendor's equipment.

  For example:

```
int e0/0
ip address 172.24.1.1 255.255.255.0
vrrp 1 ip 172.24.1.1
```

Just needs to be changed to:

```
int e0/0
ip address 172.24.1.42 255.255.255.0
standby 1 ip 172.24.1.1
standby 1 priority 254
```

- CSCtg57657

  Symptoms: A router crashes at the DHCP function.

  Conditions: This symptom is observed on a Cisco 7206VXR router running Cisco IOS Release 12.4(22)T3.

  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.

- CSCtt53985

  Symptoms: All traffic stops forwarding on a Cisco ASR 1000 series router due to the ESP crashing. Or, half entries with the IP address 239.67.33.205 may show up in the database, which may cause some end stations to be improperly translated.

  Conditions: This symptom is observed in a rare condition that can result in an ESP crash or bad half entry translations as described above.

  Workaround: For the crash, prevent SNMP from pulling NAT OIDs. This can be done by creating a view. For example:

  ```
    snmp-server view test internet included
    snmp-server view test 1.3.6.1.4.1.9.10.77.1 excluded
    snmp-server community pub view test RO
  ```

  To recover from the bad entries, a reload is required.

- CSCtw74100

  Symptoms: An issue with the PPP interface is seen upon flapping the core interfaces.

  Conditions: This symptom is observed when shut/no shut on the core interfaces is done through a script overnight, leading to a few PPP serial interfaces going up/down.

  Workaround: Shut/no shut on the serial interface resolves the issue.

- 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.

Resolved Caveats—Cisco IOS XE Release 3.4.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.2S.

- 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.

  Additional Note: This bug is fixed in Cisco IOS Release 12.2(28)SB7 via CSCsa40461.

- 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: This symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.

  Workaround: Use ASRs instead of ISR.

- 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 symptom is observed 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 the same value to the 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.

- 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: This 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.

- 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

- 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, Cisco IOS Release 15.1(3)T1, and Cisco IOS Release 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: This 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 the 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 shut down 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, causing 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, (that is, 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 a crash as 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 the **write network** command.

  Conditions: This symptom is observed when the **write network** command is used with no URL specified.

  Workaround: Specify a URL.

- CSCtq61128

  Symptoms: The router crashes with Segmentation fault (11).

  Conditions: This symptom isobserved on routers acting as the 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

- CSCtq88777

  Symptoms: The VDSL controller and ATM interface remains up; however, ATM PVC becomes inactive and virtual interface goes down.

  Conditions: This 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 the 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.

- CSCtr06926

  Symptoms: A CA server in auto grant mode goes into disabled state when it receives a client certificate enrolment request.

  Conditions: This 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.

- CSCtr35740

  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: This 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: This 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: The 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: There is no condition. But, this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr81559

  Symptoms: The PPP session fails to come up occasionally on the 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: The RP crashes sometimes when the router is having PPPoX sessions.

  Conditions: This symptom occurs 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 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.

- CSCts16013

  Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1000 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 timeout. 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.

- CSCts27042

  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

Conditions: This 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.

- 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 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.

- 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

- 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.

- 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. P
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.

- 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: This 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.

- 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.

- 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.

- 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.

- 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.

- 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 the WRED threshold become 0.

  Conditions: This 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.

- 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.

- 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.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB--RFC2833 and vice versa.

  Conditions: This symptom occurs when MTP is used to convert OOB--RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS Release XE 3.1S should work fine.

  Workaround: There is no workaround.

- CSCts76410

  Symptoms: A tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: This symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. This issue was observed with Cisco IOS Release 12.4(20)T and Cisco IOS Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCtt28703

  Symptoms: The VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored.

  Conditions: This symptom is observed when using 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

- 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: This symptom is observed with failed IKE negotiations (ph1 or ph2).

  Workaround: There is no workaround.

- CSCtt94537

  Symptoms: Auth_length of a BFD multihop packet is 0.

  Conditions: This symptom is observed when you configure BFD multihop with SHA or MD5.

  Workaround: There is no workaround.

- 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.

- CSCtv19529

  Symptoms: The router crashes on unconfiguring the last available DHCP pool. The crash is also seen on running the **no service dhcp** command.

  Conditions: This symptom can occur only if the "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.

- CSCtq68778

  Symptoms: After an ISSU, the reload reason string is missing in the newly-active session.

  Conditions: This symptom is observed after an ISSU.

  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.

- 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
  ```

Open Caveats—Cisco IOS XE Release 3.4.1S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.1S.

- CSCtr79347

  Symptoms: The 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: This symptom is observed when you change the BFD-related BGP configuration. This issue is also seen when there is no trigger.

Workaround: There is no workaround.

- CSCtr84641

  Symptoms: The misclassification issue occurs when using deny statements in the ACL for a class-map. If the packets match the deny statements, they may be not classified properly.

  Conditions: This symptom occurs when you configure deny statements in the ACL for a class-map.

  Workaround: There is no workaround.

- CSCts16013

  Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1K router. The 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.

- CSCts22958

  Symptoms: A crash occurs on the Cisco ASR-ESP when the internal memory related to fragments is exhausted.

  Conditions: This symptom occurs when the internal memory related to fragments is exhausted and a jumbo packet (larger than 16K after reassembly) is dropped by ESP.

  Workaround: There is no workaround.

- CSCts64130

  Symptoms: Tunnel MTU is incorrectly calculated when the tunnel is configured with a tunnel protection. It shows a mugh higher value than the actual value.

  Conditions: This symptom is observed on an the Cisco ASR router running Cisco IOS Release 15.1(3)S0a.

  Workaround: MTU on the egress physical interface can be lowered. However, if the tunnel is configured with “mpls ip”, there is no workaround.

- CSCts72164

  Symptoms: In a large-scale DMVPN environment using BGP as the routing protocol, a DMVPN hub router may crash in the Cisco IOS process under high- scale conditions.

  Conditions: This symptom occurs when there is a routing reconvergence in the network.

  Workaround: There is no workaround.

- CSCts82679

  Symptoms: The RP crashes on a Cisco ASR router related to crypto.

  Conditions: This symptom occurs when crypto is configured.

  Workaround: There is no workaround.

- CSCtr98684

  Symptoms: This is a rare condition triggered by the combination of using “ip ospf network point-to-multipoint” and the packet forwarding implementation on the Cisco ASR platform.

Conditions: This symptom occurs when there are OSPF adjacency issues when using the Cisco ASR router with the “ip ospf point-to-multipoint” configuration. These issues are triggered by the timing of the neighbor formation over a “shared” segment.

Workaround: Change the network type to broadcast.

Resolved Caveats—Cisco IOS XE Release 3.4.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.1S.

- 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: This symptom is observed with the following 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.

- 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: This symptom is observed with the following conditions:

  1. When the 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.

- CSCtl09030

  Symptoms: The Cisco ASR1k configured to function as ISG and DHCP relay/server crashes in the ARP input process or IP inband session initiator process in dhcpd_find_binding function.

  Conditions: This symptom is observed when the Cisco ASR1k is configured with DHCP relay or server and DHCP initiated IP sessions are configured. This issue is seen when the ISG inband IP session initiator is configured and an ARP request is received from a client whose DHCP IP session has timed out or cleared.

  Workaround: Disable ISG DHCP session initiator.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: This symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Cisco IOS Release 12.2(33)SRB and later. Earlier versions are not affected.

  Workaround: Advertise and withdraw or withdraw and readvertise a more specific prefix, which will force the reevaluation 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.

- CSCto99343

  Symptoms: Line cards do not forward packets, which causes a failure on the neighborship.

  Conditions: This symptom is observed on VSL-enabled line cards on a VSS system.

  Workaround: There is no workaround.

- CSCtq17082

  Symptoms: The router reloads.

  Conditions: This symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Vitual Template.

  Workaround: Session teardown before you remove the QoS configuration.

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: This 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: This 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.

- CSCtq79350

  Symptoms: After changing the ACL in a key server a couple of times, the rekey will fail in the GM.

  Conditions: This symptom is observed when you add/remove an ACL in a key server.

  Workaround: Use the **clear crypto GDOI** command.

- 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.

- 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: The basic IP session with dot1q encapsulation and IP initiator may not come up.

  Conditions: This symptom is observed on an ES40.

  Workaround: Reconfigure the dot1q encapsulation (which has the same VLAN ID as the outer VLAN ID of the QinQ subinterface) after an OIR.

- CSCtq96329

  Symptoms: The router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops and could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can occur 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 by performing hardreset of the BGP session to remove any stale prefixes.

  It is further recommended to do an SSO on routers that are running the impacted software to eliminate any potential corruption that might have already existed on routers that are running the impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr05003

  Symptoms: The Cisco ASR1000 with SIP calls crashes from RTPSPI.

  Conditions: This symptom is observed with H323 and SIP configurations on the router.

  Workaround: There is no workaround.

- CSCtr07704

  Symptoms: While using scripts to delete a nonexistent 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 nonexistent 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 the existing behavior, do not print out a message like “the class does not exist” when deleting a nonexistent 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.

- CSCtr18708

  Symptoms: SMI can be configured on Gigabit Ethernet0 on the Cisco ASR1k router.

  Conditions: This symptom occurs on the Cisco ASR1k router.

  Workaround: Do not configure SMI on Gigabit Ethernet0 because it is unsupported (see CSCta28011 and the SMI configuration guide).

- CSCtr19922

  Symptoms: Lots of output is printed by the **show adjacency** *[key of adj] internal dependents* command, followed by a crash.

Conditions: This 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 that 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: This symptom is observed with MPLS-TE tunnel flap.

  Workaround: There is no workaround.

- 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: This symptom is observed when you OIR the link for one LSP.

  Workaround: Shut/no shut the TP tunnel interface.

- CSCtr45608

  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: This 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: This 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 **passive-interface** command 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 the **no passive-interface** command will not form the lost OSPF ADJ.

  Conditions: This symptom is observed only with interfaces associated with the OSPF process using the **ip ospf vnet area** *number* command.

  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 **ip ospf** *process id* **area** *number* command are not affected.

- CSCtr57226

  Symptoms: The Cisco ASR router with CUBE Enterprise and the Cisco IOS SW MTPs configured can result in an MTP leak, leading to the Cisco ASR router rejecting calls with cause 47.

  Conditions: This symptom is observed when the SCCP Application process increases in memory size due to a leak. Eventually, the leaking SCCP process results in calls rejected with cause 47. The ASR CUBE must have software MTPs configured, as given below:

```
dspfarm profile x
mtp maximum sessions software y
associate application sccp
```

  The following **show** command indicates whether the SCCP Application is leaking sessions:

```
sh mem debug leak chunk
Adding blocks for GD...

                  lsmpi_io memory

Address    Size    Alloc_pc    PID    Alloc-Proc        Name

                  Processor memory
Address    Size    Alloc_pc    PID    Alloc-Proc        Name
30796D18     300    D927C74    64     IOSD ipc task     IOSD ipc task
479D651C   57140   124C946C    438    SCCP Applicatio   RTPSPI_DEQUEUE_EVENT
489C6700   57140   124C946C    438    SCCP Applicatio   RTPSPI_DEQUEUE_EVENT
48B153E0   57140   124C946C    438    SCCP Applicatio   RTPSPI_DEQUEUE_EVENT
48BE67EC   57140   124C946C    438    SCCP Applicatio   RTPSPI_DEQUEUE_EVENT
49944BFC   57140   124C946C    438    SCCP Applicatio   RTPSPI_DEQUEUE_EVENT
4A5661EC   57140   124C946C    438    SCCP Applicatio   RTPSPI_DEQUEUE_EVENT
```

  Workaround: To resolve the issue, try issuing the following commands:

```
conf t
no sccp
!
pause until SCCP cleanup is complete
sccp
end
```

  If this method is not successful, the Cisco ASR router will need to be reloaded to recover the memory from the leaked MTP sessions.

- CSCtr66878

  Symptoms: Login to Cisco ASR 1002 routers fails.

  The logs are as follows:

```
%CPPOSLIB-3-ERROR_NOTIFY: F0: fman_fp_image: fman-fp encountered an error
-Traceback= 1#78702a22f7c824a946f5ed1990873d4b errmsg:D39B000+2160
cpp_common_os:B93C000+B620 cpp_common_os:B93C000+189B8 cpp_sbs:B828000+AA98
cpp_sbs:B828000+79E4 cpp_sbs:B828000+7E1C cpp_sbs:B828000+7FC4
cpp_cef_mpls_common:BC96000+43728 cpp_cef_mpls_common:BC96000+441FC
:10000000+1C2B94 evlib:C5CF000+DABC evlib:C5CF000+FFC4 :10000000+14EF00
c:A381000+1E938 c:A381000+1EAE0
%IOSXE-6-PLATFORM: F0: cpp_cdm: Shutting down CPP MDM while client(s) still connected
%CPPHA-3-CDMDONE: F0: cpp_ha: CPP 0 microcode crashdump creation completed.
%IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP MDM while client(s) still connected
%IOSXE-6-PLATFORM: F0: cpp_ha: Shutting down CPP CDM while client(s) still connected
```

```
%PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_cdm_svr has been helddown (rc 69)
%PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process cpp_ha_top_level_server has been
helddown (rc 69)
%FMFP_QOS-6-QOS_STATS_STALLED: F0: fman_fp_image: statistics stalled
%ASR1000_OIR-6-ONLINECARD: Card (fp) online in slot F0
%IOSXE-6-PLATFORM: F0: cpp_cp: Process CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
```

The router recovers by itself.

Conditions: This symptom is observed when the Cisco ASR 1002 router is running Cisco IOS Release 12.0(1)S3 and has a zone-based firewall configured.

Workaround: Do not delete class-default from the policy map.

- 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.

- CSCti83542

  Symptoms: MPLS LDP flapping is seen with T3 SATOP CEM interface configurations.

  Conditions: This symptom is observed with T3/E3 SATOP TDM configurations.

  Workaround: There is no workaround.

- CSCto76700

  Symptoms: The multihop BFD session goes down with TE-FRR cutover.

  Conditions: This symptom may be observed with single hop, VCCV BFD, and multihop BFD sessions. However, after the TE-FRR cutover, the VCCV BF session comes back up, whereas the multihop BFD session goes down.

  Workaround: The workaround is to perform a “no shut” on the port-channel interface.

- 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.

- 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: This symptom is observed when 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: There is no workaround 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 the issue 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.

- CSCts45619

  Symptoms: T.38 Fax calls through the CUBE enterprise on the Cisco ASR platfrom with the Cisco IOS MTP colocated on the ASR can fail with cause 47 and subsequently leak a structure on the forwarding plane, causing future call failures.

  Conditions: This symptom is observed with T.38 calls through the CUBE enterprise on the Cisco ASR platform (only) with colocated MTPs in the call flow.

  Workaround: On nonredundant ASR platforms, a reload is required to clear the hung structures on the forwarding plane. On the Cisco ASR1006 with redundant RPs and ESPs, you can perform a switchover of the ESPs (FPs) to clear the problem, as follows:

```
hw-module slot F0 reload
! confirm via show platform that the F0 is in a ok, standby state, takes some
time for the F0 to reload.
sh platform
! do not execute the below command until F0 is back online
hw-module slot F1 reload
! again, confirm via show platform that the F1 is in a ok, standby state
sh platform
```

- CSCts46507

  Symptoms: Runtime Priority does not get back to the original value set as priority.

  Conditions: This symptom is observed when the tracked interface is flapped.

  Workaround: There is no workaround.

- 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
  ```

- CSCts76964

  Symptoms: The Cisco ASR router crashes with tracebacks, as given below:

  ```
  Exception to IOS Thread:
  Frame pointer 0x7F5CED910380, PC = 0x2F4A2E7

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP
  -Traceback=
  1#261f9625131701783f9129d7afdd6633 :400000+2B4A2E7 :400000+4FAFFBF :400000+4F
  BC2FB :400000+4FBC662
  :400000+371635B :400000+63E0B86 :400000+63DCB63 :400000+63F13A6 :400000+63F15
  6D :400000+629144E :4
  00000+63E51A1 :400000+64BE0B1 :400000+64BE037 :400000+63E5D59 :400000+624BB06
  :400000+63DBC34

  Fastpath Thread backtrace:
  -Traceback= 1#261f9625131701783f9129d7afdd6633 c:7F5DE3D0F000+BDDD2

  Auxiliary Thread backtrace:
  -Traceback= 1#261f9625131701783f9129d7afdd6633 pthread:7F5DE1D0E000+A7C9

  RAX = 0000000000000000 RBX = 006DE6F05C7F0000
  RCX = 0000000000000000 RDX = 0000000000000000
  RSP = 00007F5CED910380 RBP = 00007F5CED9103A0
  RSI = 0000000000000000 RDI = 4060D60A00000000
  R8 = 00000000F0466060 R9 = A038E6F05C7F0000
  R10 = 000000000AEF96B8 R11 = 8038E6F05C7F0000
  R12 = 0000000000000000 R13 = 00007F5CF0A51A80
  R14 = 4060D60A00000000 R15 = 0000000000000000
  RFL = 0000000000010246 RIP = 0000000002F4A2E7
  CS = 0033 FS = 0000 GS = 0000
  ST0 = 0000 0000000000000000 ST1 = 0000 0000000000000000
  ST2 = 0000 0000000000000000 ST3 = 0000 0000000000000000
  ST4 = 0000 0000000000000000 ST5 = 0000 0000000000000000
  ST6 = 0000 0000000000000000 ST7 = 0000 0000000000000000
  X87CW = 037F X87SW = 0000 X87TG = 0000 X87OP = 0000
  ```

```
X87IP = 0000000000000000 X87DP = 0000000000000000
XMM0 = 0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D
XMM1 = 00040000000000000000080000040001
XMM2 = 806E29E23003000000000000000000800
XMM3 = FD01000580030D028001000180010004
XMM4 = 00000000000000000000000000000000
XMM5 = 00000000000000000000000000000000
XMM6 = 00000000000000000000000000000000
XMM7 = 00000000000000000000000000000000
XMM8 = 00000000000000000000000000000000
XMM9 = 00000000000000000000000000000000
XMM10 = 00000000000000000000000000000000
XMM11 = 00000000000000000000000000000000
XMM12 = 00000000000000000000000000000000
XMM13 = 00000000000000000000000000000000
XMM14 = 00000000000000000000000000000000
XMM15 = 00000000000000000000000000000000
MXCSR = 00001F80

Writing crashinfo to bootflash:crashinfo_RP_00_00_20110308-100545-UTC
```

Conditions: This symptom is observed under the following conditions:

- GETVPN is operational on the Cisco ASR router.
- Registration to the Key-Server happens over the physical links.
- There is one primary and secondary link to the Key-Server.
- The crypto map is enabled on the primary interface first. Everything works fine here.
- The crypto map is enabled on the secondary interface .The ASR crashes as soon as you enable it on the Secondary interface with tracebacks, as shown above.
- The crash is also observed if the secondary interface is down and the crypto map is applied on it, although the crash is not observed instantly.
- The issue is also observed in Cisco IOS Release 15.1(3)Sa, along with Cisco IOS Release 12.2(33)XNE (could be reproduced only once at the first instance, and was not seen in subsequent tries) and Cisco IOS Release 12.2(33)XNF2.

When the same GDOI crypto-map is applied to two interfaces (in primary and secondary role), without the local-address configuration and TBAR enabled, and when KS sends the TBAR pseudotime update, the GM code gets confused between the two interfaces and the crash is observed. It is considered to be more of a timing issue.

Workaround 1: Disable TBAR on the Key-Server, that is, either with no replay or by changing it to counter-based to resolve the issue.

Workaround 2: Use the **crypto map** *name* **local-address** *logical-address* command globally on the Cisco ASR router and let the registration happen through the loopback .The loopback should be reachable to the Key-Server over the primary and the secondary links, respectively. Then, enable the crypto map on the primary and secondary interfaces, which will work fine.

- CSCto58710

  Symptoms: Certificate validation fails when the CRL is not retrieved.

  Conditions: This symptom is observed when a Cisco ASR 1000 series router attempts to retrieve a CRL using LDAP, and the LDAP server is in a VRF.

  Workaround: Use a certificate map to revoke certificates or publish the CRL to an HTTP server and configure “CDP override” to fetch the CRL.

Resolved Caveats—Cisco IOS XE Release 3.4.0aS

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.0aS.

- 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 orruption/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.

Resolved Caveats—Cisco IOS XE Release 3.4.0S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.4.0S.

- CSCto03123

  Symptoms:

  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

  Workaround: There is no workaround.

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

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

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

Open Caveats—Cisco IOS XE Release 3.4.0S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.4.0S.

- 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 approximately one-fourth of the total number of ISGv6 PPP sessions start flapping.

  Conditions: This issue is observed when ISGv6 PPP sessions start flapping.

  Workaround: Reload the router.

- CSCto91593

  Symptoms: Packet loss is observed after an RPSO.

  Conditions: This issue is observed after an RPSO.

  Workaround: Run the **ip multicast redundancy routeflush** command. For example:

  ```
  ip multicast redundancy routeflush maxtime 300
  ```

- CSCto93005

  Symptoms: A fatal error is observed on the ATM SPA when the **redundancy force-switchover** command is run on the peer router.

  Conditions: This issue is observed when both the following conditions are met:

  - AToM circuits are configured with a scale level of 1000 on the SPA.
  - Both like-to-like VCs and like-to-unlike VCs are configured on the SPA.

  Workaround: There is no workaround.

- CSCto93031

  Symptoms: Bulk synchronization failure is observed when the **sccp config** command is run.

  Conditions: This issue is observed when the **sccp config** command is run.

  Workaround: There is no workaround.

- CSCto98249

  Symptoms: The router crashes while re-enabling OSPFv3 on an interface.

  Conditions: This issue is observed when a large number of routes, for example, 1200000, are added.

  Workaround: There is no workaround.

- 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 an 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: The VTEMPLATE Background Mgr process crashes when QoS configurations are removed from the virtual template.

  Conditions: This issue is observed when there are at least 2000 IPSec tunnel sessions and an automated script is used to remove the QoS configurations from the virtual template.

  Workaround: There is no workaround.

- CSCtq17666

  Symptoms: Packets are dropped when the IP address is changed in the MSR.

  Conditions: This issue is observed when the IP address is changed in the MSR.

  Workaround: Reset the Vif1 interface.

- CSCtq24245

  Symptoms: If there are a large number of calls per session, new sessions do not come up due to resource shortage.

  Conditions: This issue is observed when there are a large number of calls per session.

  Workaround: There is no workaround.

- CSCtq28663

  Symptoms: The memory usage of Cisco ASR1000-SIP10 is very high and reaches the threshold value.

  Conditions: This issue is observed with four SPAs configured and the committed memory set at 91 percent.

  Workaround: There is no workaround. Note that this issue does not affect functionality.

- CSCtq31954

  Symptoms: High CPU utilization is observed during the AAA per-user process.

  Conditions: This issue is observed when there are a large number, for example, 15000, of TAL sessions.

  Workaround: There is no workaround.

- CSCtq40115

  Symptoms: The offset list does not increment the metric by the correct value.

  Conditions: This issue is observed in the EIGRP classic mode.

  Workaround: Use the EIGRP named mode.

- CSCtq46189

  Symptoms: The ESP reloads automatically.

Conditions: This issue is observed when multiple OIR operations are performed on either an individual ATM-based SPA or the SIP in which an ATM SPA is installed. Under test conditions, this issue was observed after approximately 60 OIR operations.

Workaround: Manually reload the ESP at some stage before the number of consecutive OIR operations reaches 60.

- 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: The standby SUP gets reset continuously after an SSO is performed or after the standby SUP is manually reset.

  Conditions: This issue is observed when the **archive** command is applied.

  Workaround: There is no workaround.

- CSCtq71477

  Symptoms: When the **redistribute connected metric 20000000 2 255 255 1500** command is run, the bandwdith is set to 4294967295 Kb.

  Conditions: There are no specific conditions under which this issue is observed

  Workaround: There is no workaround.

- CSCtq74691

  Symptoms: A buffer leak is observed at radius_getbuffer.

  Conditions: This issue is observed when a DHCP request is initiated from the client, following which a DHCP address is allocated from the server and a session comes up in the authenticating state. The 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: The router crashes when the **no ip trigger-authentication timeout 90 port 1** command is run.

  Conditions: This symptom is observed when the following sequence of commands is run:

  1. **ip trigger-authentication timeout 90 port 1**

2. **ethernet mac-tunnel virtual 4094**
3. **no ip trigger-authentication timeout 90 port 1**

Workaround: There is no workaround.

- CSCtq80351

  Symptoms: The SP crashes during a switchover in the RPR mode.

  Conditions: This issue is observed during a switchover in the RPR mode. The following failure and traceback messages are displayed when multicast scale configurations are performed:

```
%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 an RP reload.

  Conditions: This issue is observed when approximately 4000 crypto maps are configured. The memory leak speed depends on the session scale numbers. Session flapping increases the memory leak.

  Workaround: There is no workaround.

- CSCtq93505

  Symptoms: The SIP-200 LC crashes.

  Conditions: This issue is observed when members are swapped across bundles during VLAN allocation.

  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 less.

- CSCtq96244

Symptoms: Traceback is observed on the Cisco ASR 1004 Router when an incoming IPSec packet contains invalid SPI.

Conditions: This issue is observed when the following steps are performed:

1. The class map and policy map are configured.
2. The class map and policy map are applied to the virtual loopback tunnel router interface.
3. Traffic is started.
4. The tunnel target is changed on both the tunnel head and the tail end by shutting down the interface with the preferred route. The QoS target interface moves to the next preferred route.
5. The tunnel is changed to a new target.

Workaround: There is no workaround.

- 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.

- CSCtr10853

  Symptoms: The router crashes after running for about 10 days.

  Conditions: This issue is observed when all the following conditions are met:

  - There are 1000 or more mGRE tunnels with tunnel protection and using IKEv2.
  - Each mGRE tunnel is a BGP update source interface.

Workaround: There is no workaround.

- CSCtr12618

  Symptoms: If the ACL of a crypto map is modified, IPSec traffic stops getting forwarded until the tunnels are rekeyed.

  Conditions: This issue is observed when a crypto map is configured.

  Workaround: Run the **clear crypto session** command.

- 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.

- CSCts95579

  Symptoms: The "%CRYPTO-4-RECVD_PKT_INV_SPI" error is displayed with an unexpected/incorrect tunnel interface listed in the error message text.

  Conditions: This symptom occurs when shared tunnel protection is used. This issue is seen in a DMVPN environment.

  Workaround: There is no workaround. This is a cosmetic issue.

- CSCto58710

  Symptoms: Certificate validation fails when the CRL is not retrieved.

Conditions: This symptom is observed when a Cisco ASR 1000 series router attempts to retrieve a CRL using LDAP, and the LDAP server is in a VRF.

Workaround: Use a certificate map to revoke certificates or publish the CRL to an HTTP server and configure “CDP override” to fetch the CRL.