



Caveats in Cisco IOS XE 3.5S Releases

This chapter provides information about caveats in Cisco IOS XE 3.5S 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 3.5S Releases, page 195](#)

Caveats in Cisco IOS XE 3.5S 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 3.5S 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/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)



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

This section contains the following topic:

- [Resolved Caveats—Cisco IOS XE Release 3.5.2S, page 196](#)
- [Open Caveats—Cisco IOS XE Release 3.5.1S, page 200](#)
- [Resolved Caveats—Cisco IOS XE Release 3.5.1S, page 202](#)
- [Open Caveats—Cisco IOS XE Release 3.5.0S, page 219](#)

Resolved Caveats—Cisco IOS XE Release 3.5.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.5.2S.

- 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.
- CSCtx21589
Symptoms: The **show interface gig** command is not showing the media type information.
Conditions: This symptom is observed when executing the **show interface gig** command.
Workaround: Test SFP details 1-8 will give the media type information.
- CSCtx31201
Symptoms: PfR may have some probe missing after shut/no shut of the PfR master.
Conditions: This symptom is observed in a scale topology.
Workaround: There is no workaround.
- CSCtx35498
Symptoms: ASRNAT B2B: sessions are not aged on the active.
Conditions: This occurs when the standby stays down.
Workaround: Do not have the standby down for extended time periods.
- CSCtx37768
Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.
Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.
Workaround: Use one of the following workarounds:
 - Reload the router.
 - Remove and reapply an encapsulation configuration such as a VLAN.
 - Remove and reattach the bridge domain under the EVC.
 - Perform a **shutdown/no shutdown** on the BDI interface.

- CSCtx45774
Symptoms: The IM module crashes.
Conditions: This symptom is observed when you create a CESoPSN CEM interface.
Workaround: There is no workaround.
Further Problem Description: The IM crash leads to an IM reload. All CESoPSN connections come up in working state after this IM reload.
- CSCtx47195
Symptoms: BFD flap is seen when doing midpoint node SSO.
Conditions: This symptom is observed with BFD sessions running at 6.6ms X3 flaps when doing a soft OIR on a midpoint node through which MPLS-TP BFD sessions run. This issue is seen with 10G and 1G as the NNI interface combination.
Workaround: There is no workaround.
- CSCtx67388
Symptoms: The upstream packet does not flow in the dual-homed PE model.
Conditions: This symptom is observed when packets destined to VRRP MAC do not get redirected and forwarded out when received on the standby VRRP Gateway.
Workaround: There is no workaround.
- CSCtx70505
Symptoms: The 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 the **show platform software peer chassis-manager fp standby** command periodically.
Workaround: Reload the router.
- 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.

- CSCtx94393

Symptoms: ESP crashes at fman_avl_free.

Conditions: This symptom is observed with the following conditions:

- Scale IKEv2 4k IPsec sessions with the FlexVPN dVTI server.
- Scale IKEv1 1k IPsec sessions with the dVTI server.
- CAC (50) enabled on both the server and client.
- DPD (60/15/on-demand) enabled.
- Do a **clear crypto session** per 20 minutes on the server.
- 20M bidirectional traffic.

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.

- 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 symptom has only been observed on either ESP40 forwarding cards or on a Cisco ASR 1001 router. This issue 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.

- CSCty31732

Symptoms: Ping fails to the peer end that has a port-channel with member links on different niles. OSPF neighbourship is also not established.

Conditions: This symptom is observed with a port-channel in the core that has member links on different niles.

Workaround: Flap (shut/no shut) the port-channel member links.

- CSCty35010

Symptoms: Interface counters are not proper in the **show interface** command

Conditions: Abnormal interface counters are observed on interfaces that have service-instances configured under them. Also **show interface port-channel** packet in and packet out counters are not equal to the sum of the counters on each member.

Workaround: There is no workaround.

- CSCty43582

Symptoms: The **port-channel load-balance-hash-algorithm** CLI is not saved properly in the running configuration.

Conditions: This symptom is observed when the hash algorithm chosen is one of src-ip, dst-ip, or src-dst-ip.

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.

- CSCty48439

Symptoms: The **show interface BDI** CLI stats do not increment.

Conditions: This symptom is seen under all conditions.

Workaround: Use the **show platform hardware pp active interface statistics bdi** command to track only valid IPv4 multicast/unicast packets via input and output counts.

- 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.

- CSCty57746

Symptoms: On the Cisco ASR 903 router, the **show environment** command displays incorrect values, including P0 and P1 voltages and Amps values.

Conditions: This symptom is observed with the Cisco ASR 903 router when you apply the **show environment** command.

Workaround: There is no workaround.

- CSCty62559

Symptoms: On the Cisco ASR 1000 series router, FP crash occurs at `cpp_qm_obj_add_to_parent` with 8k xconnects.

Conditions: This symptom is observed with the Cisco ASR 1000 series router while doing SPA reload after RP switchover with 8k xconnects.

Workaround: There is no workaround.

- CSCty62887

Symptoms: When more than 1024 DTL requests are made during free sip msg_info pool, the Cisco ASR 1000 router will crash.

Conditions: Multiple factors could contribute to this. It depends on the number of messages contained in SIP ALG.

Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.5.1S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.5.1S.

- CSCtx11665

Symptoms: There is a memory leak in the “HTTP CORE” process. Use the **sh proc mem sort** command to determine the process using the most memory and decode it.

Conditions: This symptom is observed when the default profile is configured on the router, that is, Smart Call Home is enabled.

Workaround 1: In the Smart Call Home profile, use the email transport method to send xml format to backend server. This method needs an available mail server. The reference configuration is below:

```
Router#show run | sec call-home
service call-home
call-home
contact-email-addr <email address>
mail-server xxx.xx.xxx.xxx priority 1
profile "<profile name>"
active
```

Workaround 2: Disable the default profile so that Smart Call Home is disabled, and then use the http address instead of the https address.

- 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.

- CSCtx25459

Symptoms: An ESP module of a Cisco router may unexpectedly reload due to an exception on the QFP.

Conditions: This symptom is observed when the WCCP connection is reset on a Cisco ASR router configured with WCCP.

Workaround: Disable WCCP.

- CSCtx25926

Symptom: BPDU forwarding stops working on an EOMPLS pseudowire.

Conditions: This symptom is observed in a pseudowire after a change in its core interface.

Workaround: Re-configure the EVC-xconnect.

- 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.

- CSCtx32973

Symptoms: A Cisco router crashes due to stack corruption.

Conditions: This symptom is observed when preemption is seen with the “BFD PP Process” from the crash file similar to the following:

Preempted processes context:

Proc name: BFD PP Process	Preempted PC: 0x6DEF54
Proc name: BFD PP Process	Preempted PC: 0x6DEBB4
Proc name: BFD PP Process	Preempted PC: 0x6DEF54
Proc name: BFD PP Process	Preempted PC: 0x28232D0
Proc name: BFD PP Process	Preempted PC: 0x28232D0
Proc name: BFD PP Process	Preempted PC: 0x6DEB7C
Proc name: BFD PP Process	Preempted PC: 0x6DEBD0
Proc name: BFD PP Process	Preempted PC: 0x2823280
Proc name: BFD PP Process	Preempted PC: 0x6FC970
Proc name: BFD PP Process	Preempted PC: 0x282316C

Workaround: There is no workaround.

- CSCtx37768

Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.

Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.

Workaround: Use one of the following workarounds:

- Reload the router.
- Remove and reapply an encapsulation configuration such as a VLAN.
- Remove and reattach the bridge domain under the EVC.
- Perform a **shutdown/no shutdown** on the BDI interface.

- CSCtx41849

Symptoms: A Cisco RP1 crashes during a crypto SS process.

Conditions: This symptom is observed with the following message under the conditions listed below:

```
Ixia -- CES (IPSec static crypto map) -- UUT (IPSec DVTI server)
UUT - 4RU(RP1/ESP10)
```

- Scale 1000 IKE * 1 Vrf * 4 IPSec, total 4K IPSec sessions.
- CAC [30] is enabled.
- DPD [60/15/on-demand] is enabled.
- Reload CES (7200 platform) every 10-15 minutes.
- 60M bidirectional traffic.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.5.1S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.5.1S.

- 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.

- CSCsb53810

Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

Conditions: This issue is under investigation.

Workaround: Reload the switch.

- CSCsg48725

Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

```
TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
```

Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCtg57657

Symptoms: A router is crashing at dhcp function.

Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

Workaround: There is no workaround.

- CSCtg58029

Symptoms: After switchover, **aaa_acct_session_id** command is not issued to new sessions.

Conditions: This symptom occurs only after switchover.

Workaround: There is no workaround.

- CSCtj64807

Symptoms: 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 sub-interface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtk00181

Symptoms: Password aging with crypto configuration fails.

Conditions: This symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.

Workaround: There is no workaround.

- 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.

- CSCtn02208

Symptoms: Old PerUser ACL not removed on applying new ACL.

Conditions: This symptom occurs when applying a new PerUser ACL to an existing session. The old PerUser ACL that exists on the session is not removed.

Workaround: There is no workaround.

- CSCtn40771

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

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

Workaround: There is no workaround.

- 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.

- 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 the interface using the **ip routing protocol purge interface** command.

- CSCtr08680

Symptoms: The following error messages are displayed on active and standby respectively:

```
%ERROR: Standby doesn't support this command
BERT is running on this channel group, please abort bert first.
```

Conditions: This symptom is observed when trying to create a channel after BERT has been started irrespective of whether BERT is running or completed.

Workaround: There is no workaround.

- CSCtr45551

Symptoms: T1/E1 controller does not get selected as network clock input source.

Conditions: This symptom occurs when **network-clock input source t1/e1** command is configured immediately after reload of the router or within 5 minutes from router bootstrap.

Workaround: After the router reloads, wait for 5 to 6 minutes (until SETS gets initialized) and then configure T1/E1 as network clock input source.

- CSCtr47642

Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best-external** command, a specific prefix may not have bestpath calculated for a long time.

Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

1. Configure: **bgp additional-paths install** under VPNv4 AF.
2. Configure: **bgp additional-paths select best-external**.

Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr88739

Symptom 1: The 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.

- 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>

- CSCts00341

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

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

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

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

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

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

- CSCts13255

Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

```
%CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
heartbeats
```

Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE -- this includes 15.0S, 15.1S and 15.2S. This doesn't affect RSP 720.

Workaround: There is no workaround.

- CSCts23882

Symptoms: ISG calculates the radius response authenticator in CoA account-profile-status-query replies wrongly, resulting in an invalid response.

Conditions: This symptom is observed when the CoA/WWW based session authentication is triggered via a CoA account logon using the "old" SSG command attributes.

Workaround: Configure a fix "NAS-IP-Address" value with the **radius-server attribute 4** *x.x.x.x* command.

- 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>

- 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 **show flow monitor top** top-talkers command.

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

- 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** command 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.

- 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>

- CSCts85694

Symptoms: The following error message is displayed:

```
%FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi (0x104C2E4)
```

Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak increases incrementally. Leak is very slow.

Workaround 1: Do not bring down all sessions together.

Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

Workaround 3: Do not have accounting accuracy configured.

Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts97124

Symptoms: Active crashes upon configuring a large number of TP tunnels with scale configurations either using copy paste or loading from a configuration file.

Conditions: This symptom is not very consistent, not reproducible all the time, and happens only on adding tunnel TP configurations. The crash occurs when the protect-lsp is being configured.

Workaround: Manually add the MPLS-TP tunnels through CLI instead of copying from a configuration or copy pasting a large configuration.

- 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.

- CSCtt01056

Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

- In case of service activation from Access-Accept, the session should be terminated.
- In case of service activation from COA, the COA should be NAKed, and the services rolled back.

Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

Workaround: There is no workaround.

- 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.

- CSCtt02645

Symptoms: CPUHOG is seen due to flapping of all NHRP.

Conditions: This symptom is observed with scaling to 3k spokes on RP1.

Workaround: There is no workaround.

- CSCtt04448

Symptoms: There is a loss of IGMP snooping entries with a traffic drop at the pmLACP PoA boxes occurring.

Conditions: This symptom is observed when removing/re-adding member links.

Workaround: There is no workaround.

- CSCtt11210

Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

The "debug crypto isakmp" debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

Conditions: This symptom is observed when the router does not have the Root CA certificate installed.

Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- 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.

- CSCtt26643

Symptoms: A Cisco ASR 1006 router running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

Conditions: This symptom is observed on a Cisco ASR 1006 router running the “asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin” image. The **show version** command causes the “Last reload reason: Critical software exception” error.

Workaround: There is no workaround.

- CSCtt28703

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

Conditions: This symptom is observed if RSA-SIG is used.

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

- CSCtt29615

Symptoms: Any CLI command issued under af-interface mode in EIGRP router may lead to router crash.

Conditions: This problem is observed in a Cisco router that is running Cisco IOS Release 15.2(1)S.

Workaround: There is no workaround.

- CSCtt31634

Symptoms: Traffic drops.

Conditions: This symptom occurs when the hw-module reloads the IM on active and posts which switchover is performed.

Workaround: After switchover, use the **hw-module subslot reload** command to recover from the problematic state, and traffic will resume.

- 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.

- CSCtt43843

Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

Conditions: It is occurring with a Cisco 7200 platform loaded with the 15.2 (1.14)T0.1 image.

Workaround: There is no workaround.

- CSCtt45536

Symptoms: “FlowVar-Chunk malloc failed” messages are seen and this may be accompanied by slow console response.

Conditions: This symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.

Workaround: There is no workaround.

- CSCtt45654

Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

Workaround: There is no workaround.

- CSCtt70585

Symptoms: IPv6 traffic is not flowing.

Conditions: This symptom is seen with IPSec v6 tunnels.

Workaround: There is no workaround.

- CSCtt95846

Symptoms: Changing the encapsulation of an Ethernet service instance which is set up for local switching to default encapsulation may cause an error in setting up switching, resulting in an inability to switch packets.

```
PE1#show running-config | include local  
connect local Ethernet0/0 1 Ethernet1/0 1  
PE1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
PE1(config)#interface Ethernet0/0
```



```

PE1(config-if)#service instance 1 ethernet
PE1(config-if-srv)#encapsulation default
PE1(config-if-srv)#end
PE1#show ssm id
SSM Status: No switches

```

Conditions: This symptom is observed if **no aaa new-model** command is configured.

Workaround: Unconfigure the local switching connection before changing the encapsulation of the service instance, then reconfigure the connection.

- 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 using the **no application redundancy** command.

- CSCtu02286

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

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

Workaround: Use non pim-bidir modes.

- CSCtu12574

Symptoms: The **show buffers** command output displays:

1. Increased missed counters on EOBC buffers.
2. Medium buffer leak.

```

Router#sh buffers
Buffer elements:
    779 in free list (500 max allowed)
    1582067902 hits, 0 misses, 619 created

Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
    273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
    0 in free list (0 min, 2400 max allowed)
    2400 hits, 161836 fallbacks
    1200 max cache size, 129 in cache
....

```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTs tracks the leak specific to IPC application l3-mgr.

```

From the <CmdBold>show buffers old pack</noCmdBold> output:
0A9C4ED8: 00200000 02150000 0202080B 01000000 . . . . . --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A .T.....I>M..|.
0A9C4EF8: 00520002 00000000 00000000 00000000 .R..... --> ICC Header
-- --

```

And, if we look at the ICC header at the underscored items 00520002:

```

0052    (represents the class name)          ----> L3_MGR_DSS_REQUESTS
0002    (represents the request name)        ----> L3_MGR_MLS_REQ

```

Workaround: Reload the system.

- CSCtu18201

Symptoms: A Cisco router crashes due to low stack with the following display:

```
%SYS-6-STACKLOW: Stack for process BGP Event running low, 0/6000
```

Conditions: This symptom occurs with a low stack.

Workaround: There is no workaround.

- CSCtu19450

Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu29729

Symptoms: An attempt to create a frame-relay sub-interface on a serial interface may result in error. The serial interface can then not be configured as a frame-relay interface.

Conditions: This symptom is observed when a serial interface is configured as a multi-link frame-relay bundle link with a subsequent attempt to change the configuration to a frame-relay interface.

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.

- CSCtu35713

Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

Conditions: This symptom is observed under the following conditions:

1. Enable IPv4 address saving on BRAS.
2. Configure AAA periodic accounting using the **aaa accounting update periodic time in mins** command.
3. Initiate IPCP negotiation from the client.
4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic time in mins**.

- CSCtu36674

Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

Workaround 1: Perform shut/no shut on local connect.

Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu39819

Symptoms: The Cisco ASR 1002 router configured as an RSVP Agent for Cisco Unified Communication Manager crashes under extended traffic.

Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVP Agent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

The image used is “asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin”.

Workaround: There is no workaround.

- CSCtu41137

Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

Conditions: The core is observed while doing unconfiguration.

Workaround: There is no workaround.

- CSCtu43731

Symptoms: On an RP1, RP switchover causes an RP reset.

Conditions: This symptom is observed with RP switchover under the following conditions:

- The router must be an RP1.
- The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

Workaround 2: Do not enable FNF monitoring.

- CSCtu87383

Symptoms: CFM global configuration does not get applied to LC slots that are greater than 20 on LC OIR. This problem is specific to CPT platform where satellite box slot numbers go from 36 to 55.

Conditions: This symptom occurs with satellite box OIR.

Workaround: Disable and reenable CFM global configuration.

- CSCtu89771

Symptoms: The Cisco ASR 1000 series router RP crashes while unconfiguring or removing the **no area 0 authentication ipsec spi <>** command.

This behavior is not observed at the first few instances of unconfiguring the above CLI.

Conditions: This symptom is observed only in automated tests where unconfiguring the authentication with the above CLI is executed multiple (approximately 3) times on the Cisco ASR 1000 series router. This leads to the RP crashes.

Workaround: There is no workaround.

- CSCtu92213

Symptoms: Console is stuck and unresponsive.

Conditions: This symptom is seen when EVC with QoS is scaled, and traffic is being sent through many policy-maps with a large queue limit.

Workaround: Configure a smaller queue-limit under each class on all egress policy-maps in use.

- CSCtu92289

Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

Workaround: There is no workaround.

- CSCtu92673

Symptoms: L2TP tunnels are not getting established with PPPoE relay.

Conditions: This issue is seen on a Cisco 7200 router that is running Cisco IOS Interim Release 15.2(01.12)S.

Workaround: There is no workaround.

- CSCtv19529

Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

The client process can be started:

1. from an DHCP autoinstall attempt during router startup (with no nvram config).
2. if the **ip address dhcp** is run on one of the interfaces.

3. if the router was used for DHCP proxy client operations.

The relay processes are started when a DHCP pool is created by the **ip dhcp pool pool** command.

Workaround: Have a dummy DHCP pool created using the **ip dhcp pool dummy_pool** command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw43640

Symptoms: An IP ping/CFM session through Handoff FPGA fails.

Conditions: This symptom is observed after switchover with IM in slot 5.

Workaround: There is no workaround.

- CSCtw45055

Symptoms: A Cisco ASR router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
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 dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

Workaround: There is no workaround.

- CSCtw45168

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

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

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 CEsPs 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 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.

- CSCtw50277

Symptoms: Policy manager is getting apply config failed on standby while policy is activated through CoA. The router later crashes in policy code.

Conditions: This symptom is seen when CoA activated policy install is failing on standby RP.

Workaround: There is no workaround.

- CSCtw51134

Symptoms: IMA interface configuration is lost post stateful switchover (SSO).

Conditions: This symptom occurs after SSO.

Workaround: There is no workaround.

- CSCtw52504

Symptoms: WAN mode is not enabled on 10G IMs.

Conditions: This symptom is observed when a 10G IM operates in LAN mode by default. The WAN mode supports SONET alarms to interface with SONET-like equipments.

Workaround: There is no workaround.

- CSCtw52610

Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure using the **max-xmit-utilization percentage 100** command.

- CSCtw58395

Symptoms: When executing the **clear crypto session** command in 4k FlexVPN cases, the memory of crypto IKEv2 is increasing.

Conditions: This symptom is observed when the session is flapping.

Workaround: There is no workaround.

- CSCtw58586

Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPsec profile default. This enhancement request will change the behavior and create an automatic anchorage.

Conditions: This symptom is seen in IKEv2 usage.

Workaround: There is no workaround.

- CSCtw64040

Symptoms: Crash due to MPLS, which appears to be associated with load-balancing.

Conditions: This symptom occurs when MPLS is configured.

Workaround: There is no workaround.

- CSCtw68745

Symptoms: A Cisco ASR 1000 router acting as DHCPv6 Relay standby crashes when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

Conditions: This symptom occurs when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

Workaround: There is no workaround.

- CSCtw73551

Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

```
UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps
```

Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.

Workaround: There is no workaround.

- CSCtw76044

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

Conditions: This symptom is observed under all conditions.

Workaround: There is no workaround.

- CSCtw79579

Symptoms: Standby fails to be in standby HOT state after reload.

Conditions: This symptom is seen after removal of an IM and doing RSP stateful switchover (SSO) and then trying to bring up the standby RSP.

Workaround: There is no workaround.

- CSCtw85883

Symptoms: The error “ace_add_one_map failed” occurs while adding an ACE to a crypto acl that is being used by a crypto map.

Conditions: This symptom is observed when the crypto map is applied to an interface and the crypto acl being modified is also in use.

Workaround: Remove the crypto map and apply the ACL changes to avoid the error.

- CSCtw94319

Symptoms: Crash is seen at dhcpd_forward_request.

Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- 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.

- CSCtw99877

Symptoms: IOMD process on 10G IM crashes upon booting standby.

Conditions: This symptom is observed when the interface state is down on active.

Workaround: There is no workaround.

- CSCtx01604

Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx05942

Symptoms: The session to the service module from the Supervisor Fails. This can happen with SAMI, NAM, NAM-2 etc. modules.

For example, if the SAMI card is in Slot 2, the **session slot 2 processor 0** command fails to create a telnet session and fails to give out the following messages:

```
SUP#session slot 2 proc 3
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.33 ...
% Connection timed out; remote host not responding
```

Conditions: This symptom occurs with 15.2(1)S release. It is not observed with Cisco IOS Release 15.1(3)S1 or lower version.

Workaround: Downgrading the Supervisor to Cisco IOS Release 15.1(3)S1 or lower version resolves this issue.

- CSCtx09614

Symptoms: With the preconfigured ATM configuration, the standby RSP does not boot up.

Conditions: This symptom is observed when one of the RSPs is up and the running configuration has the ATM configuration under the controller.

Workaround: There is no workaround. Without an ATM configuration, the standby RSP goes to standby mode.

- CSCtx21206

Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1.

Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- 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 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 insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- CSCts29892

Symptoms: The **mtu** command is not allowed on BDI interfaces on the Cisco ASR 903 router.

Conditions: This symptom occurs when you configure the **mtu** command on BDI interfaces.

Workaround: There is no workaround. However, note that the **ip mtu** command is supported on BDI interfaces.

Open Caveats—Cisco IOS XE Release 3.5.0S

This section documents the unexpected behavior that might be seen in Cisco IOS XE Release 3.5.0S.

- CSCtg68047

Symptoms: The router reloads.

Conditions: This symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

Workaround: Wait until the tunnels are shut down before issuing the show command.

- CSCtj58706

Symptoms: On executing ISSU runversion, the standby RP reloads multiple times before reaching hot-standby.

Conditions: This symptom is observed during ISSU upgrade/downgrade with the iso1-iso2 image. This issue is seen with scaled configuration of 7000 L2VPN, 300 BGP, 300 EIGRP, and 8000 EVC sessions.

Workaround: There is no workaround.

- 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.

- CSCtn83900

Symptoms: After performing legacy mode or native mode subpackage ISSU with flexible NetFlow configured, the interface to monitor bindings may not be present on the newly active RP.

Conditions: This symptom is observed when a legacy mode or native mode subpackage ISSU is performed with FNF configured.

Workaround: Remove the FNF monitors prior to the subpackage ISSU. Add the monitors back to the interface configuration after the upgrade. Alternatively, use super-package ISSU, which does not have this limitation.

- 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.

- CSCtq80891

Symptoms: The Processor Pool for the Cisco IOS memory is used up with most of the buffers in the “IPv6 PIM input queue”.

Conditions: This symptom is observed with the following topology:

IXIA [IPv6 Mcast Source] ----- TR1 (ASR1k) -----|500 IPv6 over IPv4 GRE

Tunnels | ----- UUT (ASR1k) [IPv6 RP] ----- |500 IPv6 over IPv4 GRE

Tunnels | ----- TR2 (7200) ----- IXIA [IPv6 Mcast MLD Hosts]

- 500 IPv6 Sources sending Mcast traffic to 500 IPv6 Mcast groups
- 500 PIM-RP on UUT
- 500 PIM-RP Acl to make sure 1 Mcast-group/Tunnel
- The GRE tunnels could be configured with tunnel protection or not.

The reproduce procedure is as follows:

1. Copy configurations (IPv6 over IPv4 GRE Tunnel Protections and IPv6 Mcast included) to TR1, TR2, and UUT.
2. Launch Mcast traffic (500M) on IXIA.
3. Hit the Cisco IOS memory depletion issue on UUT.

Workaround: Configure the punt policer for PIM register packets as follows:

platform punt-policer 55 limit-number

platform punt-policer 55 limit-number high

The limit-number above is a number between 1000-2000.

- CSCtr80274

Symptoms: CISCO-LICENSE-MGMT-MIB does not populate.

Conditions: This symptom occurs when the required license is installed on the Cisco ASR 903 router, but the SNMP query does not return any value.

```
ASR903#show license
```

```
Index 1 Feature: metroaggrservices
      Period left: Life time
      License Type: Permanent
      License State: Active, In Use
      License Count: Non-Counted
      License Priority: Medium
Index 2 Feature: metroipservices
      Period left: 8 weeks 4 days
      License Type: Evaluation
      License State: Active, Not in Use, EULA not accepted
      License Count: Non-Counted
      License Priority: None
Index 3 Feature: metroservices
      Period left: 8 weeks 4 days
      License Type: Evaluation
      License State: Active, Not in Use, EULA not accepted
      License Count: Non-Counted
      License Priority: None
```

```
sw-mrrbu-nms-2:2> getmany 3.3.2.11 ciscoLicenseMgmtMIB
```

```
sw-mrrbu-nms-2:3>
```

Workaround: There is no workaround.

- CSCts05124

Symptoms: A zero-byte crash file is generated upon a crash with TREX SPA.

Conditions: This symptom is observed with a test crash on a SIP-400 line card with TREX SPA inserted.

Workaround: There is no workaround.

- CSCts11715

Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

Workaround: There is no workaround.

- CSCts12499

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

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

Workaround: There is no workaround.

- CSCts13255

Symptoms: Standby SUP crash is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

%CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive heartbeats

Conditions: This symptom is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is also seen with Cisco IOS Release 12.2(33)SRE.

Workaround: There is no workaround.

- CSCts47550

Symptoms: When applying protocol attributes policy rules, traceback may be seen.

Conditions: This symptom is not consistent and may or may not appear when applying the protocol attributes policy rules. This symptom is also not consistent with a specific protocol, but may appear with respect to different protocols.

Workaround: There is no workaround.

- CSCts63426

Symptoms: With 1K EoMPLS PWs, 6 percent performance drop is observed in Cisco IOS XE Release 3.5 compared to Cisco IOS XE Release 3.4 performance.

Conditions: This symptom is observed with 1K EoMPLS PWs in Cisco IOS XE Release 3.5.

Workaround: There is no workaround.

- CSCts63658

Symptoms: Multicast traffic do not flow over EVCs on the port-channel.

Conditions: This symptom is observed during router reload.

Workaround: Reconfigure after the router reload. Configure regular EFPs before EFPs on the PC in the same BD.

- CSCts82598

Symptoms: Incorrect IP from the NAT pool is chosen for translation, when one protocol exhausts all ports of all IPs and another protocol traffic is received.

Conditions: This symptom occurs when one protocol (for example, TCP) exhausts all ports of all IPs in a pool, and only one IP from the pool is selected for translation, thus limiting the capacity of creating translations. This happens only when one protocol completely exhausts all ports and then another protocol traffic starts. This usually is not the case in customer environments that mostly see both TCP and UDP traffic hitting the box time.

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.

- CSCtt01056

Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

- In case of service activation from Access-Accept, the session should be terminated.
- In case of service activation from COA, the COA should be NAKed, and the services rolled back.

Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

Workaround: There is no workaround.

- CSCtt02645

Symptoms: CPUHOG is seen due to flapping of all NHRP.

Conditions: This symptom is observed with scaling to 3k spokes on RP1.

Workaround: There is no workaround.

- CSCtt04724

Symptoms: On PPPoEoX, when activating multiple services from Access-Accept with long Cisco-SSG-Account-Info strings, if the aggregated string length exceeds the current limit of 256 characters, then the service activation fails, a traceback is seen, and the session is allowed to establish, no services will be applied in the ingress and/or egress directions.

Conditions: This symptom is observed when the aggregated services string length exceeds the limit (256 characters).

Workaround: The session should be terminated instead. In case of service activation from CoA, if the cumulative services string length exceeds the limit, then the last CoA should be NAKed, and the services rolled back to the previous state.

- CSCtt11210

Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.

The "debug crypto isakmp" debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.

Conditions: This symptom is observed when the router does not have the Root CA certificate installed.

Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt11558

Symptoms: The Cisco ASR 1000 router displays the "INVALID_GPM_ACCESS" error message due to invalid GPM load. This may cause unexpected Embedded Services Processors (ESP) reload.

Conditions: This symptom is observed when a small packet is sent from a BDI interface to an Ethernet service instance with either the **rewrite egress tag** command or the **rewrite ingress tag** command with the **symmetric** option present.

Workaround: There is no workaround.

- CSCtt21257

Symptoms: After a reload or switchover, all interfaces on one or more IMs may be down down. The state of the IMs is "ok, active", which is shown in the **show platform** command output.

Conditions: This symptom is occasionally observed after a reload or a switchover.

Workaround: Power cycle the box.

- CSCtt26532

Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

Workaround: There is no workaround.

Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt33937

Symptoms: Configure port 7 on the Gigabit IM as a port to forward traffic using IP routing.

```
config t
interface g0/0/7
ip address 10.0.0.1 255.255.255.0
```

Conditions: This symptom is observed when traffic is flowing well. When you perform a switchover, and once the standby becomes the new active, the traffic does not hit the ingress counter of the interface itself. On checking the links status using the registers, the SGMI link appears out of sync.

Workaround: There is no workaround. Reload the box when this symptom is observed.

- CSCtt34361

Symptoms: During a soak test with 1800 PPPoE sessions flapping with the IPv4 Saving feature enabled + per-user ACLv4 and ACLv6, there is no ISG service. After 56 iterations, one memory snapshot is taken every four iterations, that is, roughly 270 seconds per iteration. The test duration is 4 hours, with total 100800 sessions established with an average of 7cps.

Conditions: This symptom occurs under the following conditions:

1. No active session is there in the router.
2. Establish 1800 PTA dual-stack sessions with per-user ACL from Radius + IPV4 Saving feature.
3. Wait till all sessions come UP.
4. Take a memory leak snapshot “high”.
5. Wait for all sessions to time out on the Idle timer (no traffic).
6. Wait for all sessions to go DOWN.
7. Take a memory snapshot.
8. Loop back to 1.

Workaround: There is no workaround.

- CSCtt45654

Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

Workaround: There is no workaround.

- CSCtt45801

Symptoms: The DMVPN HUB RP crashes with the default EIGRP timer when scaling to 4k spokes.

Conditions: This symptom occurs when scaling to 4k spokes.

Workaround: Changing the EIGRP timer to longer may reduce the chances of a crash.

- 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.

- CSCtt70346

Symptoms: IOMD crash is seen when running the PTP session.

Conditions: This symptom is observed when running the PTP session for a long time. Sometimes, this issue is seen when changing PTP packet rates. This issue is seen rarely.

Workaround: There is no workaround.

- CSCtt70498

Symptoms: After a reload or switchover, the state of F0 or F1 may become “disconnecting” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding RSP does not forward traffic.

Conditions: This symptom is occasionally observed after a reload or a switchover.

Workaround: Power cycle the box.

- CSCtt94147

Symptoms: Nile manager crash is observed.

Conditions: This symptom is observed with the following conditions:

- VPLS in the core.
- REP in the access.
- The access-side REP segment flaps a few times.

Workaround: There is no workaround.

- CSCtt94566

Symptoms: The router crashes before all sessions come up.

Conditions: This symptom occurs before all sessions come up.

Workaround: There is no workaround.

- CSCtt95577

Symptoms: After creating the 994th VC on a T1/E1 IM on the Cisco ASR 903 router, the traffic flow stops. Packets get dropped on the egress on the router.

Conditions: This symptom is observed when ping starts to fail on all the pre-existing VCs upon adding the 994th VC. The working is unaffected till 993 VCs.

Workaround: Delete the 994th VC to make the pre-existing VCs forward traffic.

- CSCtt97164

Symptoms: If the router interface is flapped, the HSRP message may be dropped by the punt/inject path.

Conditions: This symptom is seen if the router interface is flapped.

Workaround: Disable the inject bypass.

- CSCtt97473

Symptoms: After a reload or switchover, the RSP may reset during bootup.

Conditions: This symptom is observed occasionally after a reload or switchover.

Workaround: There is no workaround.

- CSCtt98574

Symptoms: After a reload or switchover, the state of one or more IMs may become “out of service” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding interfaces do not come up.

Conditions: This symptom is occasionally observed after a reload or a switchover.

Workaround: Power cycle the box.

- CSCtt99235

Symptoms: After a switchover, an IOMD process crashes because it has failed to establish LIPC connection.

Conditions: This symptom is seen occasionally after a switchover.

Workaround: Reload the box.

- CSCtu02280

Symptoms: When running the PTP session for an extended period of time, there is a very small likelihood of PTP daemon crashing.

Conditions: This symptom occurs when running the PTP session for a long time.

Workaround: There is no workaround.

- CSCtu02476

Symptoms: An SSO followed by a change in the xconnect MTU results in the pseudowire in the redundant RP to go down. The pseudowire in the Active RP remains up and running. A subsequent SSO results in the pseudowire to go down.

Conditions: This symptom is observed with “encapsulation default” at that end of the pseudowire where SSO is performed. An SSO followed by a change in the MTU value, and then a subsequent SSO, causes the pseudowire to go down. This issue is also seen in a setup with redundant pseudowires, where the primary and backup pseudowires configured under the service instance do not come up after changing the MTU with SSO.

Workaround: Execute “no xconnect” under the service instance, and then reconfigure the pseudowire with the new MTU value under the service instance.

- CSCtu03699

Symptoms: The Nile Manager crashes.

Conditions: This symptom is observed when reloading the TP tunnel endpoint multiple times.

Workaround: There is no workaround.

- CSCtu12574

Symptoms: The **show buffers** command output displays:

1. Increased missed counters on EOBC buffers.
2. Medium buffer leak.

```
Router#sh buffers
```

```
Buffer elements:
```

```
779 in free list (500 max allowed)
```

```
1582067902 hits, 0 misses, 619 created
```

```
Interface buffer pools:
```

```
....
```

```
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
```



```

00:01:17):
    273 in free list (64 min, 3000 max allowed)
EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
    0 in free list (0 min, 2400 max allowed)
    2400 hits, 161836 fallbacks
    1200 max cache size, 129 in cache
....

```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

The DDTS CSCtr34960 tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```

0A9C4ED8: 00200000 02150000 0202080B 01000000 . . . . . -----> IPC
Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A .T.....I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000 .R..... ----->
ICC Header
-- --

```

And, if we look at the ICC header at the underscored items 00520002:

```

0052 (represents the class name) -----> L3_MGR_DSS_REQUESTS
0002 (represents the request name) -----> L3_MGR_MLS_REQ

```

Workaround: Reload the system.

- CSCtu13806

Symptoms: Upon switchover, the “red_switchover_process” process causes a crash on the old active RSP.

Conditions: This symptom is observed upon switchover.

Workaround: This crash is harmless as another RSP becomes active and works properly. Reboot the RSP to make it come up as standby.

- 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.

- CSCtu17006

Symptoms: Mediatrace is not working because RSVP fails to select the output interface.

Conditions: This symptom is observed only with PFR configuration.

Workaround: Remove the PFR configuration.

- CSCtu17296

Symptoms: Traffic failure occurs on 3 to 4 VLANs out of 1000.

Conditions: This symptom is observed after reloading the UUT.

Workaround: Remove and readd the service instance configuration for the affected VLANs.

- CSCtu17540

Symptoms: IOMD core is generated on switchover for T1/E1 IM. After switchover, the IOMD process is aborted.

Conditions: This symptom is observed with every switchover.

Workaround: There is no workaround.

- CSCtu18150

Symptoms: FP crash occurs due to a wrong FCID handling issue.

Conditions: This symptom occurs due to a wrong FCID handling issue.

Workaround: There is no workaround.

- CSCtu24765

Symptoms: Under scale (28.8K PPPoX sessions), when executing “show policy-map session” from the CLI, both ESPs crash.

Conditions: This symptom is observed with a large scale, that is, 28K PPPoE sessions established + ISG QoS services.

Workaround: There is no workaround.

- CSCtu27601

Symptoms: On ATM BRAS under scale (16K PPPPoEOA sessions + ISG services), the ESP crashes occasionally during sessions establishment.

Conditions: This symptom is observed with a large scale (16K PPPPoEOA sessions + services).

Workaround: There is no workaround.

- CSCtu28990

Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

Workaround: There is no workaround.

- CSCtu29047

Symptoms: After a reload or switchover, the RSP may exhibit a kernel hang.

Conditions: This symptom is observed occasionally after a reload or switchover.

Workaround: Power cycle the box.

- CSCtu32935

Symptoms: IPv6 traffic loss of around 30 seconds is seen for routes learned from dynamic routing protocols upon RSP switchover with the Nonstop Forwarding (NSF) configuration. IPv6 CEF is not programmed on the standby RSP.

Conditions: This symptom is observed with RSP switchover.

Workaround: There is no workaround for the dynamic routing protocol. Problem will not be seen for static route.

- CSCtu33258

Symptoms: LDP over MPLS-TP tunnel fails to get established upon router reload.

Conditions: This symptom is seldom seen when the router is reloaded with scaled MPLS-TP tunnels that have LDP session established over the tunnels. Pinging traffic through the tunnel fails.

Workaround: There is no workaround.

- CSCtu34906

Symptoms: All ptp sessions go down on the BC upon configuring more than 63 slaves to negotiate with it.

Conditions: This symptom is observed on the BC when there are more than 63 slaves trying to negotiate with the master. This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master, but only with the BC master.

Workaround: This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master.

- CSCtu35713

Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

Conditions: This symptom is observed under the following conditions:

1. Enable IPv4 address saving on BRAS.
2. Configure AAA periodic accounting using the **aaa accounting update periodic time in mins** command.
3. Initiate IPCP negotiation from the client.
4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic time in mins** command.

- CSCtu41497

Symptoms: The Nile Manager crashes.

Conditions: This symptom is observed with a 256 rmep scale.

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.

- CSCtv22685

Symptoms: The ESP on the Cisco ASR 1000 router crashes or the GRE tunnel does not switch over when the destination interface is removed or the route changes, causing the tunnel interface to stop forwarding packets.

Conditions: This symptom is observed when multiple GRE tunnels are configured on the same interface(s) with a high traffic rate across the tunnels.

Workaround: Only configure one GRE tunnel per physical interface.

- CSCtu98727

Symptoms: ANCP shaping with Model F fails with BRR classes.

Conditions: This symptom is observed with BRR classes, but works fine with LLQ (priority level) classes.

Workaround: There is no workaround.

- CSCtv14686

Symptoms: When a hierarchical policy with more than one VLAN class uses the same child policy, such as an HCoS policy will not work and the support will be tracked via CSCtw44894.

Conditions: This symptom is observed when a hierarchical policy with more than one VLAN class uses the same child policy.

Workaround: Ensure that there is a different child policy-map attached to each VLAN class. The child policy-maps could have the same content, but needs to have different policy-map names.

- 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.

- CSCts33401

Symptoms: When the Cisco ASR 903 router has multiple heterogeneous ECMP paths for routing a MPLS packet to the destination, for example, one path through MPLS routing and the other through IP routing, if the IP path comes before the MPLS path in the load balance object, the Cisco ASR 903 fails to forward the MPLS packet in the hardware. The MPLS packet is either dropped or punted to Cisco IOS for routing. If the MPLS path comes before the IP path in the load balance object, MPLS packets are forwarded by the Cisco ASR 903 hardware.

In addition, there is no issue if the incoming packet is an IP packet, even though there are multiple heterogeneous ECMP paths to reach the destination. The same issue also exists in the Whales platform for routing MPLS packets when there are multiple heterogeneous ECMP paths to reach the destination.

Conditions: This symptom is observed with heterogeneous ECMP paths for routing an MPLS packet to the destination.

Workaround: There is no workaround.

- 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.